Cadre de gestion des incidents de confidentialité

Commissaire à la santé et au bien-être
19 janvier 2023
Mise à jour no 1 – 24 septembre 2025

Cadre de gestion des incidents de confidentialité

Table des matières

1. Objectifs

Ce document a pour but d'établir le cadre de gestion des incidents de confidentialité du CSBE. Il précise entre autres les étapes à suivre pour le traitement d'un incident de confidentialité ainsi que les rôles et responsabilités des différents intervenants impliqués, et rappelle les principales obligations du CSBE en lien avec la déclaration et l'enregistrement des incidents de confidentialité.

2. Champ d'application

Ce cadre de gestion s'applique à l'ensemble du personnel du CSBE, y incluant les étudiants et les stagiaires, et à toute personne ou entité qui transige avec le CSBE, que ce soit à titre de mandataire ou de prestataire de services.

Il s'applique à tout renseignement personnel et tout renseignement de santé et de services sociaux détenu par le CSBE ou par un tiers pour son compte, et ce, durant tout son cycle de vie, c'est-à-dire l'ensemble des étapes que franchit le renseignement et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du CSBE.

3. Assises légales

L'obligation pour un organisme public de se doter d'un cadre de gestion des incidents de confidentialité est apparue en septembre 2022 avec l'entrée en vigueur des premières dispositions modifiant la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, ci-après « Loi sur l'accès », instituées par le chapitre 25 des Lois du Québec 2021 (ci-après « Loi 25 »).

Près de deux années plus tard, soit le 1er juillet 2024, est entrée en vigueur la nouvelle *Loi sur les renseignements de santé et de services sociaux* (c. R-22.1), prévoyant des obligations similaires quant à la gestion d'incidents de confidentialité impliquant des renseignements de santé ou de services sociaux (RSSS).

Rappelons que ces derniers renseignements sont des renseignements personnels, mais qui bénéficient d'un régime de protection particulier établi par cette nouvelle loi.

Les dispositions à consulter, pour assurer un traitement des incidents de confidentialité conforme aux exigences légales applicables en la matière, sont les suivantes :

Loi sur l'accès	LRSSS
• Articles **63.8** à **63.11**, **127.2** et **158**; • Règlement sur les incidents de confidentialité (c. A-2.1, r. 3.1)[1]	• Articles **108** à **110**.

Comme les deux lois prévoient des dispositions très similaires, nous les présentons plus loin (section 3.2), sous forme de tableau comparatif pour en faciliter l'appropriation. Les nuances nécessaires seront apportées au besoin.

3.1. Qu'est-ce qu'un incident de confidentialité?

Selon l'article **63.9** de la Loi sur l'accès, un « incident de confidentialité » consiste en :

1) l'accès non autorisé par la loi à un renseignement personnel;

2) l'utilisation non autorisée par la loi d'un renseignement personnel;

3) la communication non autorisée par la loi d'un renseignement personnel;

4) la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

La LRSSS ne définit pas cette notion. Ainsi, aux fins de l'application du présent cadre de gestion, cette définition s'applique à tout incident de confidentialité, qu'il vise un renseignement personnel ou un RSSS.

Plus largement, et tel que défini dans la politique organisationnelle du CSBE en matière d'accès à l'information et de protection des renseignements personnels (ci-après « la Politique »), l'incident de confidentialité s'entend de « [t]*oute divulgation non autorisée d'information confidentielle (par exemple, un renseignement personnel ou un RSSS), et ce, peu importe le support sur lequel elle se trouve (papier, clé USB, ordinateur, tablette numérique, téléphone intelligent, etc.) et tout accès non autorisé à une telle information. Ces bris peuvent être intentionnels ou accidentels. Ils peuvent résulter d'une erreur humaine ou de la défaillance d'un système. Selon la Loi sur l'accès et la LRSSS, un incident de confidentialité peut résulter d'un accès non autorisé à un renseignement personnel*

[1] Adopté le 30 novembre 2022. Selon le décret no 1761-2022 du gouvernement du Québec, publié à la Gazette officielle du Québec, 14 décembre 2022, 154e année, no 50, pp. 6819-6822. Le Règlement est entré en vigueur le 15e jour suivant ladite publication, soit le 29 décembre 2022.

ou à un RSSS, d'une utilisation ou d'une communication non autorisée d'un tel renseignement ou de toute autre atteinte à sa protection incluant sa perte ».

3.2. Principales exigences et obligations à respecter

Comme mentionné plus haut, les exigences édictées par les deux lois sont très similaires et l'intention du législateur semblait claire, dans la LRSSS, à l'effet de répliquer les principes énoncés dans la « Loi 25 » à l'égard des incidents de confidentialité.

Précisons que pour le moment, aucun règlement spécifique n'a été adopté par le gouvernement relativement aux articles 108 à 110 de la LRSSS, de sorte que le CSBE devrait donc suivre les instructions fournies par le Règlement sur les incidents de confidentialité pour déterminer les actions à poser et les informations à fournir, advenant un incident de confidentialité.

Le tableau suivant présente les exigences à respecter par le CSBE à l'égard du traitement d'un incident de confidentialité, en fonction du type de renseignement concerné (personnel ou RSSS).

Exigences à respecter à l'égard du traitement d'un incident de confidentialité

Exigence à respecter par le CSBE	Loi sur l'accès	LRSSS
Prendre les mesures raisonnables pour mitiger les risques d'un préjudice sérieux lorsqu'il a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel / un RSSS s'est produit et éviter qu'une telle situation se reproduise	Art. **63.8**, al. 1	Art. **108**, al. 1

• Dans son évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, considérer, notamment :
  ○ la sensibilité du renseignement concerné;
  ○ les conséquences appréhendées de son utilisation;
  ○ et la probabilité qu'il soit utilisé à des fins préjudiciables.
• Consulter la personne responsable de la protection des renseignements personnels au sein de l'organisation.
	Art. **63.10**	Art. **109**

Aviser la Commission d'accès à l'information (CAI) s'il estime que l'incident risque de causer un préjudice sérieux.	Art. **63.8**, al. 2, Règlement sur les incidents de confidentialité, art. 3 (informations à transmettre à la CAI)	Art. **108**, al. 2 Dans un tel cas, le CSBE doit aussi aviser le ministre de la Santé. *Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus à l'article 108. **Aucun règlement adopté à ce jour.
Aviser toute personne dont un renseignement personnel / un RSSS est concerné par l'incident si celui-ci présente un risque de préjudice sérieux.	Art. **63.8**, al. 2; Règlement sur les incidents de confidentialité, art. 5 (informations à transmettre à ces personnes);	Art. **108**, al. 2

Exigence à respecter par le CSBE	Loi sur l'accès	LRSSS
	Idem, art. 6 (dans quels cas le CSBE devrait-il donner un avis public de l'incident de confidentialité).	
Aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.	Art. **63.8**, al. 2 C'est un **pouvoir** et non une obligation. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.	Art. **108**, al. 2 C'est un **pouvoir** et non une obligation.
Se doter d'un registre des incidents de confidentialité	Art. **63.11;** Règlement sur les incidents de confidentialité, art. 7 (informations à inscrire dans un tel registre)	Art. **110** Un règlement du gouvernement peut déterminer la teneur de ce registre. Aucun règlement adopté à ce jour.
Garder à jour et conserver les renseignements qu'il contient, à l'égard d'un incident de confidentialité, durant une période minimale de 5 ans à compter du moment où il a pris connaissance de cet incident.	Règlement sur les incidents de confidentialité, art. 8	

Le texte complet des dispositions de la Loi sur l'accès et de la LRSSS est reproduit aux annexes 1 et 2.

4. Contexte organisationnel

Le mandat du CSBE est défini à l'article 2 de sa loi constitutive (*Loi sur le Commissaire à la santé et au bien-être*, RLRQ, c. C-32.1.1, ci-après « LCSBE »), et ses pouvoirs et responsabilités sont énoncés dans cette même loi, tel que plus amplement décrit dans la Politique.

Le CSBE ne rend pas de services directs à la population et n'administre pas de programmes ou de mesures impliquant des interactions directes avec les citoyens. Ainsi, dans le cadre de ses activités de mission, hormis ceux qui sont nécessaires à l'exercice de ses responsabilités administratives (ressources humaines, gestion contractuelle, etc.), il ne recueille pas de renseignements personnels (sauf ceux décrits aux paragraphes ci-dessous). Son rôle, en tant qu'organisme jouant un rôle-conseil auprès du ministre de la Santé (« le ministre »), est plutôt d'apprécier la performance globale du système québécois de santé et de services sociaux, d'un point de vue systémique, et de formuler au ministre des recommandations en vue d'améliorer cette performance.

Dans ce contexte, le CSBE doit travailler avec des données, de diverses natures et provenant de sources variées, par exemple : revues de littérature, consultation d'experts et d'autres acteurs clés du système de santé et de services sociaux, consultations auprès des citoyens (y compris par des sondages), y incluant les membres du Forum de consultation, et consultation des banques de données populationnelles notamment, détenues par d'autres organisations du domaine de la santé et des services sociaux.

Ainsi le CSBE doit, dans le cadre de ses travaux, accéder à des données, dont certaines contiennent des renseignements personnels et des RSSS, qui se retrouvent dans ses bases de données sous une forme dépersonnalisée ou anonymisée. Ainsi, le CSBE doit s'assurer du respect des cadres légaux et réglementaires applicable à ces renseignements de nature confidentielle. Il doit également offrir, aux organisations qui lui permettent d'avoir accès à leurs données, les meilleures garanties en ce qui concerne la consultation, l'utilisation, la communication, la conservation et la destruction de ces données.

Par ailleurs, en plus d'accéder à une importante quantité de données renfermant des renseignements personnels ou de santé et de services sociaux, le CSBE travaille avec de nombreux partenaires externes, aux intérêts parfois divergents, et, de ce fait, se trouve dépositaire de quantités d'information sensible.

5. Définitions[2]

Renseignement personnel

Renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier, c'est-à-dire de la distinguer d'une autre personne.

Ce peut être notamment, mais de manière non limitative, un renseignement relatif à l'identité (nom, prénom[3] , date de naissance, numéro d'assurance sociale, numéro de permis de conduire, etc.), un renseignement à caractère financier (information sur les comptes bancaires, numéro de carte de crédit, etc.), une caractéristique d'une personne (origine ethnoculturelle, religion, expérience de travail, scolarité, etc.), la photographie ou la vidéo d'une personne ou encore ses données biométriques (empreintes digitales, iris, voix, etc.). Un tel renseignement ne peut être communiqué sans le consentement de la personne concernée, sauf dans les cas d'exception permis par la loi.

Renseignement personnel sensible

Tel que mentionné à l'article 59 de la Loi sur l'accès, un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attente en matière de vie privée. Le renseignement peut être de nature médicale, biométrique ou autrement intime, ou être considéré sensible en raison du contexte de son utilisation ou de sa communication.

Les renseignements portant sur les allégeances individuelles ou protégés par la *Charte des droits et libertés de la personne* (RLRQ, chapitre C-12), dont les renseignements sur la religion, l'orientation sexuelle ou les allégeances politiques, sont sensibles.

Un renseignement sensible ne peut être communiqué sans le consentement exprès de la personne concernée, sauf dans les cas d'exception permis par la loi.

Renseignement de santé et de services sociaux (RSSS)

L'article 2 de la LRSSS définit le RSSS comme tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes :

[2] Les trois définitions énoncées dans ce cadre de gestion sont tirées de la politique organisationnelle du CSBE en matière d'accès à l'Information et de protection des renseignements personnels.

[3] Suivant l'article 56 de la Loi sur l'accès, le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

1) il concerne l'état de santé physique ou mentale de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne ;

2) il concerne tout matériel prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant ou toute orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne ;

3) il concerne les services de santé ou les services sociaux offerts à cette personne, notamment la nature de ces services, leurs résultats, les lieux où ils ont été offerts et l'identité des personnes ou des groupements qui les ont offerts ;

4) il a été obtenu dans l'exercice d'une fonction prévue par la *Loi sur la santé publique* (c. S-2.2) ;

5) toute autre caractéristique déterminée par règlement du gouvernement.

De plus, un renseignement qui permet d'identifier une personne, par exemple, son nom, sa date de naissance, ses coordonnées ou son numéro d'assurance maladie, est un RSSS s'il est accolé à un RSSS ou s'il est recueilli aux fins d'enregistrer, d'inscrire ou d'admettre la personne concernée dans un établissement de santé ou pour sa prise en charge par un organisme du secteur de la santé et de services sociaux.

6. Traitement d'un incident de confidentialité

Cette section décrit le traitement d'un incident de confidentialité par le CSBE lorsque celui-ci a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel ou un RSSS s'est produit.

Les principes qui y sont énoncés sont alignés, notamment, sur les règles proposées par la CAI[4] en cas de survenance d'un incident de confidentialité, y incluant la perte ou le vol de renseignements personnels, en tenant compte des exigences prescrites par la loi. Le CSBE suit également le schéma de traitement d'un incident de confidentialité élaboré par le ministère du Conseil exécutif[5]. Celui-ci est reproduit à l'annexe 3.

[4] Source : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-ministeres-et-organismes-publics/incidents-confidentialite-impliquant-renseignements-personnels_organismes.

[5] Source : En ligne, https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1642792255

6.1. Évaluation sommaire de la situation

Au CSBE, tout employé, prestataire de services ou mandataire alerté de la survenance réelle ou potentielle d'un incident de confidentialité, ou impliquée dans un tel incident, doit amorcer sans délai la réalisation d'une évaluation de la situation. Ainsi, elle doit, seule ou avec les autres personnes alertées ou impliquées :

a) définir sommairement le contexte de l'incident, en identifiant :

- les renseignements personnels ou les RSSS visés par l'incident et leur support, ainsi que les personnes affectées, leur nombre et leur groupe (employés, mandataires, membres du Forum de consultation, etc.) ;
- le contexte des événements (date, heure, lieu, etc.) ;
- si possible, les circonstances de l'incident (cause, personnes susceptibles d'être impliquées dans l'incident, etc.) ;
- les mesures de sécurité physiques et informatiques en place lors de l'incident.

b) Informer le secrétaire général, qui informera le commissaire et évaluera, avec la personne responsable de la protection des renseignements personnels (RPRP) la situation et au besoin, la nécessité d'informer les autorités externes concernées de l'incident, ainsi que l'urgence de le faire selon les circonstances, et ce, parfois même avant l'évaluation des risques de préjudice sérieux, telles que :

- les services informatiques du ministère de la Santé et des Services sociaux ;
- le service de police, si les circonstances indiquent ou laissent supposer qu'un crime a été commis ;
- la CAI ;
- le ministre (s'il s'agit d'un RSSS).

Le secrétaire général désignera une personne ou une équipe responsable de la gestion de la situation, selon la gravité et l'ampleur de l'incident.

6.2. Limitation de l'atteinte à la vie privée

Dès la survenance d'un incident de confidentialité, le CSBE prend sans tarder, s'il y a lieu, des mesures adéquates afin de limiter les conséquences, pour les personnes concernées, d'une possibilité d'utilisation malveillante de leurs renseignements personnels ou de leurs RSSS, ou encore de l'usurpation ou du vol de leur identité, à savoir :

a) faire le nécessaire pour limiter sans délai les conséquences d'un accès, d'une utilisation ou d'une communication non autorisés de renseignements personnels ou de RSSS, ou d'une perte ou d'un vol de ces renseignements, en s'assurant de mettre fin à la pratique non conforme le cas échéant ;

b) récupérer les dossiers physiques ou numériques, selon le cas ;

c) révoquer ou modifier les mots de passe ou les codes d'accès informatiques ;

d) contrôler les lacunes dans les systèmes de sécurité.

6.3. Évaluation des risques

Après avoir réalisé les actions prioritaires et urgentes ci-dessus, le CSBE procède à l'évaluation des risques que l'incident de confidentialité cause un préjudice sérieux aux personnes concernées. L'évaluation doit comporter les étapes suivantes :

a) compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels ou des RSSS en cause et en tenant compte notamment de leur nature, de leur quantité, des conséquences appréhendées de leur utilisation, de la possibilité qu'ils soient utilisés à des fins préjudiciables ainsi que de la possibilité de les combiner avec d'autres renseignements, ce qui pourrait permettre d'identifier les personnes concernées par ces renseignements;

b) déterminer le contexte de l'incident, en s'intéressant notamment aux éléments suivants :

- la cause (par exemple, s'agit-il d'un geste délibéré ou d'un accident, d'une erreur humaine, d'une faille informatique, etc.) ;
- les auteurs connus ou probables d'un accès, d'une utilisation ou d'une communication non autorisée de renseignements personnels ou de RSSS, ou de la perte ou du vol de ces renseignements (par exemple, une organisation criminelle, le public en général, etc.) ;

- l'étendue de la situation (nombre de personnes touchées, secteurs touchés) ;
- le caractère systémique ou non d'un accès, d'une utilisation ou d'une communication non autorisés de renseignements personnels ou de RSSS, ou de la disparition de ces renseignements (en particulier lorsque la perte n'est pas générée directement par une intervention humaine) ;
- une évaluation de la probabilité qu'un événement similaire se reproduise ;

c) évaluer la possibilité que les renseignements personnels ou les RSSS concernés fassent l'objet d'une utilisation susceptible de nuire aux personnes concernées en tenant compte, entre autres, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.) ;

d) évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels ou les RSSS ;

e) évaluer si les mesures immédiates qui ont été prises étaient adéquates pour limiter l'atteinte, et les compléter si nécessaire ;

f) déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels ou des RSSS par des personnes malveillantes, notamment pour le vol d'identité ;

g) déterminer les priorités et les actions à prendre sur la base des résultats de l'évaluation ainsi réalisée.

6.4. Avis aux personnes et organismes concernés

Une fois l'évaluation des risques effectuée,

a) le CSBE détermine qui doit être mis au courant de l'accès, de l'utilisation ou de la communication non autorisée de renseignements personnels ou de RSSS, ou la perte ou du vol de ces renseignements, en fonction de son évaluation des risques, notamment, lorsqu'un incident présente un risque qu'un préjudice sérieux soit causé :

- le service de police : lorsque la disparition peut résulter de la commission d'un crime, le service de police concerné doit d'abord être informé des éléments entourant cette disparition, puis de toutes les démarches

subséquentes. On doit prendre garde à ne pas nuire à l'enquête et veiller à préserver les éléments de preuve qui pourraient être pertinents ;

- les personnes concernées : si l'accès, l'utilisation ou la communication non autorisé(e) de renseignements personnels ou de RSSS, ou la perte ou le vol de ces renseignements risque de leur causer préjudice, celles-ci devraient en être avisées sans tarder, afin qu'elles puissent prendre les mesures nécessaires pour protéger leurs renseignements personnels ou leurs RSSS. Les informations à transmettre à ces personnes, ainsi que l'énoncé des situations où un avis public devrait être donné, sont précisés à la section III (articles 5 et 6) du Règlement sur les incidents de confidentialité ;

- la CAI, si l'accès, l'utilisation ou la communication non autorisée de renseignements personnels ou de RSSS, ou la perte ou le vol de ces renseignements risque de causer des préjudices sérieux aux personnes concernées par ces renseignements. La CAI pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solutions. Le formulaire prescrit par la CAI peut être utilisé pour informer cette dernière de la survenance d'un incident de confidentialité[6] ;

- le ministre, s'il s'agit de RSSS;

- autres : selon les circonstances, il pourrait aussi être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc. Toutefois, en leur fournissant des informations au sujet de l'incident de confidentialité, on doit veiller à ne pas aggraver le préjudice que pourraient subir les personnes concernées (par exemple, limiter au minimum les renseignements personnels ou les RSSS fournis dans les avis).

b) le CSBE désigne les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone) ;

[6] Ce formulaire est adapté suivant les exigences de l'article 3 du Règlement sur les incidents de confidentialité, qui énonce les informations à transmettre à la CAI. L'article 4 de ce même Règlement prévoit en outre que l'organisme doit transmettre à la CAI tout renseignement énoncé à l'article 3 porté à sa connaissance après la transmission de l'avis visé à ce même article et ce, avec diligence.

c) s'il y a lieu, il consigne par écrit les motifs justifiant sa décision de ne pas aviser les personnes concernées et les autres intervenants.

Un aide-mémoire pour guider la démarche d'avis aux personnes et organismes concernés est reproduit à l'annexe 4.

6.5. Inscription au registre des incidents de confidentialité

Tout incident de confidentialité doit être inscrit au registre des incidents de confidentialité du CSBE, y compris les incidents ne présentant pas de risque qu'un préjudice sérieux soit causé. La personne ou l'équipe responsable de la gestion de la situation ou de l'incident doit transmettre les informations nécessaires à la personne responsable de la PRP, qui effectue l'inscription au registre.

6.6. Évaluation approfondie et prévention

Après avoir posé les gestes à caractère plus urgent identifiés plus haut, le CSBE doit réaliser une évaluation plus approfondie de l'incident, dans un souci de prévention et d'amélioration de ses façons de faire. Plus précisément, il doit :

a) approfondir l'analyse des circonstances de l'incident et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés ;

b) répertorier et examiner son cadre normatif (normes, politiques ou directives internes) en place au moment de l'incident, autant sur les plans de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels ou des RSSS en général ;

c) vérifier si ce cadre normatif a été suivi par les personnes impliquées (et déterminer les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant) ;

d) s'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter ses processus pour éviter qu'un tel incident se reproduise ;

e) évaluer la nécessité de se doter d'un énoncé de politique et/ou de règles plus spécifiques en matière de traitement d'un accès, d'une utilisation ou d'une communication non autorisés de renseignements personnels ou de RSSS, ou d'une perte ou d'un vol de ces renseignements ;

f) formuler des recommandations relatives à des solutions à moyen et à long terme et à d'éventuelles stratégies de prévention, s'il l'estime nécessaire ;

g) s'assurer de la réelle nécessité de la collecte des renseignements personnels ou des RSSS concernés ;

h) s'assurer du suivi devant être accordé, notamment en ce qui concerne :

- le processus de traitement qui doit être appliqué lors d'un accès, d'une utilisation ou d'une communication non autorisés de renseignements personnels ou de RSSS, ou d'une perte ou d'un vol de ces renseignements et les résultats obtenus, afin de l'améliorer, s'il y a lieu ;
- les mesures de sécurité requises à la suite de l'incident et leur performance ;
- la communication de l'information pertinente à la CAI, au service de police impliqué, s'il y a lieu, ainsi qu'au ministre s'il s'agit d'un RSSS.

7. Rôles et responsabilités

Au CSBE, les rôles et responsabilités, en matière d'accès à l'information et de protection des renseignements personnels, sont définis dans la Politique.

Plus spécifiquement lors d'un incident de confidentialité,

7.1. La personne impliquée dans celui-ci ou alertée de la survenance réelle ou potentielle d'un tel incident

a) elle procède à l'évaluation sommaire de la situation ;

b) elle informe le secrétaire général ;

c) elle collabore avec le ou les responsables de la gestion de l'événement, le secrétaire général et la personne responsable de la PRP tout au long du processus.

7.2. Le secrétaire général

a) il informe la personne responsable de la PRP ;

b) il détermine, avec cette dernière s'il y a lieu, le partage des responsabilités pour les suites à donner ;

c) il désigne la personne ou l'équipe responsable de la gestion de la situation ;

d) il informe les intervenants concernés à l'interne.

7.3. La personne (l'équipe) responsable de la gestion de la situation

a) elle collabore avec le secrétaire général, notamment quant au partage des responsabilités pour les suites à donner ;

b) elle prend au besoin les mesures adéquates afin de limiter les conséquences, pour les personnes concernées, d'une possibilité d'utilisation malveillante des renseignements personnels ou des RSSS ; au besoin, elle sollicite la collaboration de la RPRP ;

c) elle transmet à la personne responsable de la PRP les informations nécessaires à l'inscription de l'incident au registre des incidents de confidentialité du CSBE.

7.4. La personne responsable de la protection des renseignements personnels (PRP)

a) En cohérence avec ses responsabilités telles qu'énoncées dans la Politique, elle coordonne la mise en œuvre, l'application et la mise à jour du présent cadre de gestion, en collaboration avec le directeur de l'administration ;

b) En collaboration avec le secrétaire général,

- elle évalue la nécessité d'informer les autorités externes concernées ;
- elle procède à l'évaluation des risques de préjudice sérieux ;
- elle détermine, sur la base de son évaluation, qui doit être mis au courant d'un accès, d'une utilisation ou d'une communication non autorisés de renseignements personnels ou de RSSS, ou de la perte ou du vol de ces renseignements, et selon quelles modalités ;
- elle réalise *a posteriori* une évaluation plus approfondie de l'incident ;
- elle inscrit l'incident au registre des incidents de confidentialité ;

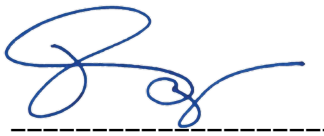
c) elle fournit à ce dernier, ainsi qu'à toute autre personne impliquée dans un incident de confidentialité, son soutien et son expertise de pointe en matière de protection des renseignements personnels et des RSSS ;

d) elle offre de façon générale son soutien et son expertise à l'ensemble du personnel du CSBE, notamment par des activités de sensibilisation et de formation, en ce qui a trait aux incidents de confidentialité.

8. Adoption et entrée en vigueur

Les modifications au présent cadre de gestion entrent en vigueur le jour de leur adoption.

Signé à Québec ce 24e jour de septembre 2025



_____

Joanne Castonguay, commissaire

ANNEXE 1

Dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1) relatives aux incidents de confidentialité
(articles **63.8** à **63.11**)

« **63.8.** Un organisme public qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser la Commission. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Il peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.

Malgré le deuxième alinéa, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.

63.9. Pour l'application de la présente loi, on entend par "incident de confidentialité" : 1° l'accès non autorisé par la loi à un renseignement personnel ; 2° l'utilisation non autorisée par la loi d'un renseignement personnel ; 3° la communication non autorisée par la loi d'un renseignement personnel ; 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

63.10. Lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, un organisme public doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation

et la probabilité qu'il soit utilisé à des fins préjudiciables. L'organisme doit également consulter son responsable de la protection des renseignements personnels.

63.11. Un organisme public doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre. Sur demande de la Commission, une copie de ce registre lui est transmise. »

Cliquez sur le lien pour accéder au Règlement sur les incidents de confidentialité.

ANNEXE 2

Dispositions de la *Loi sur les renseignements de santé et de services sociaux* (RLRQ, chapitre R-22.1) relatives aux incidents de confidentialité
(articles **108** à **110**)

« **108.** Un organisme qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement qu'il détient ou qu'un tel incident risque de se produire doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et pour éviter que de nouveaux incidents de même nature ne se produisent.

Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser le ministre et la Commission d'accès à l'information. Il doit également aviser toute personne dont un renseignement est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Il peut également aviser toute personne ou tout groupement susceptible de diminuer ce risque et lui transmettre, sans le consentement de la personne concernée, tout renseignement nécessaire à cette fin.

Malgré le deuxième alinéa, une personne dont un renseignement est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un groupement qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois.

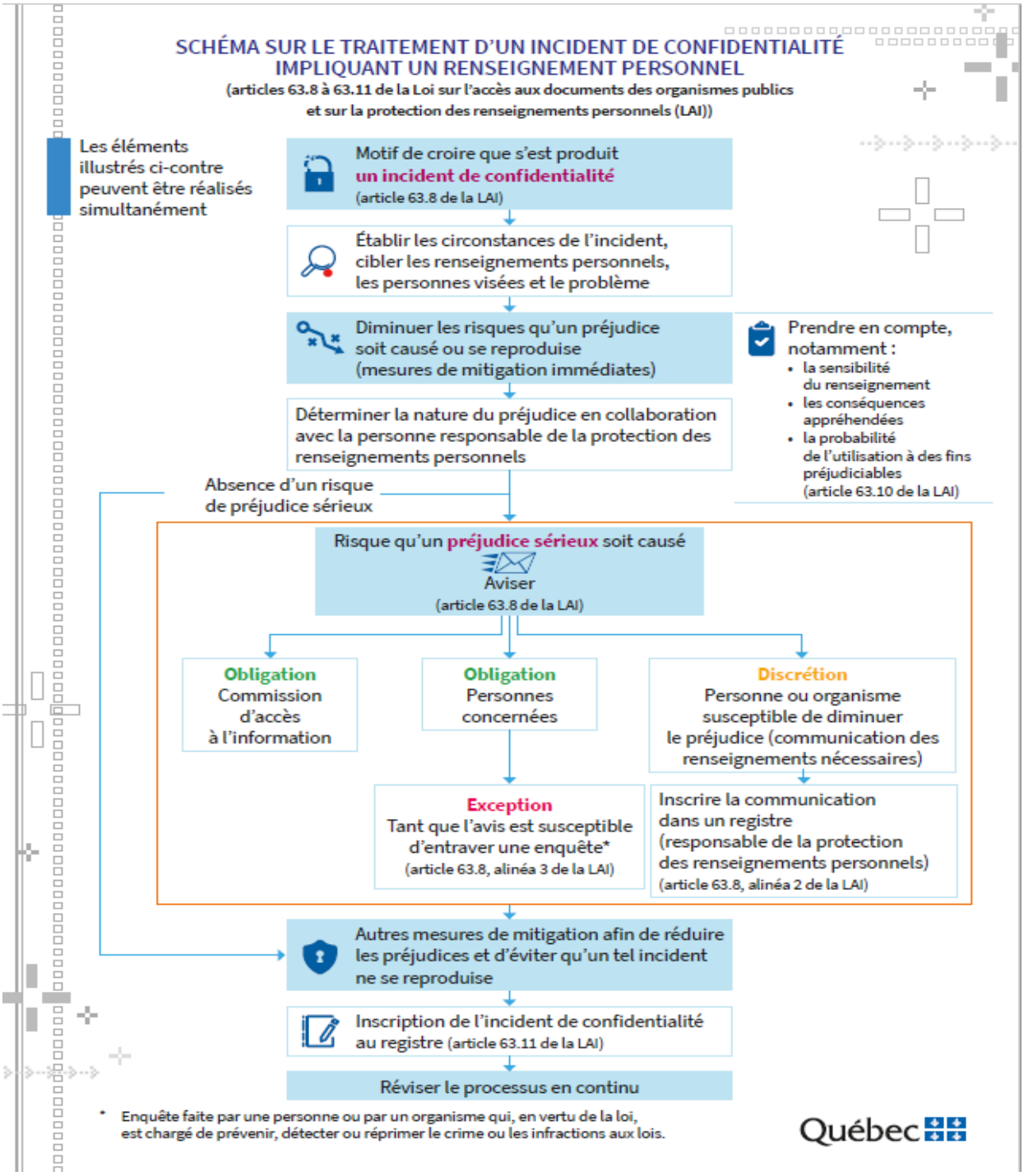
Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.

109. Lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement est concerné par un incident de confidentialité, un organisme doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. L'organisme doit également consulter son responsable de la protection des renseignements.

110. Un organisme doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre.

Sur demande du ministre ou de la Commission d'accès à l'information, une copie de ce registre lui est transmise. »

ANNEXE 3



Source
[En ligne], https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1642792255

ANNEXE 4

AVIS AUX PERSONNES CONCERNÉES
PAR UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT
LEURS RENSEIGNEMENTS PERSONNELS OU LEURS RSSS :

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels. Cet avis pourrait inclure certains des éléments suivants :

- le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques ;
- une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (service de police, Commission d'accès à l'information, etc.) ;
- les actions prises par les organismes et les entreprises pour aider les personnes concernées (service d'aide et d'information, abonnement à une alerte de crédit, etc.) ;
- les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger (référence au document « Le vol d'identité en bref ! »[7] disponible sur le site Internet de la Commission d'accès à l'information);
- les autres documents d'information générale conçus pour aider les personnes à se prémunir contre le vol d'identité;
- les coordonnées d'un interlocuteur de l'organisation qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement;
- les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, formation du personnel, révision ou élaboration de politiques, vérification, suivi périodique, etc.).

[7] Source : *Perte ou vol de renseignements personnels : comment réagir?* Aide-mémoire à l'intention des citoyens (https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FIC_Vol_RP_Citoyens.pdf)