Confidentialité

Politique et pratiques encadrant la gouvernance des renseignements personnels

cap santé mentale
Confédération des associations de proches en santé mentale du Québec

Document officiel adopté par le conseil d'administration le 30 janvier 2024

Confédération des associations de proches en santé mentale du Québec
219-1990, rue Cyrille-Duquet
Québec (Québec) G1N 4K8
Tél. : 418 687-0474 / info@capsantementale.ca
www.capsantementale.ca

Afin d'éviter les redondances qui surchargeraient le texte, l'usage du masculin dans cette politique est utilisé comme genre neutre pour désigner à la fois les femmes et les hommes et a pour unique but d'alléger le texte.

CAP santé mentale remercie la Table des regroupements provinciaux d'organismes communautaires et bénévoles (TRPOCB) et la COCQ-SIDA de lui avoir partagé ses outils et connaissances et de lui avoir permis de s'en inspirer pour la création de cette politique.

TABLE DE MATIÈRES

ARTICLE 1 - Objet de la politique

La présente politique a pour objet d'offrir un cadre de protection des renseignements personnels détenus par la Confédération des associations de proches en santé mentale du Québec (ci-après nommée « CAP santé mentale »). Elle répond aux nouvelles obligations de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* qui a été sanctionnée le 22 septembre 2021 afin, notamment, d'offrir un meilleur contrôle aux citoyens sur leurs renseignements personnels et d'être mieux adaptée à la réalité technologique d'aujourd'hui.

CAP santé mentale respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements personnels recueillis auprès de toute personne participant à ses activités et à toute personne qu'elle emploie. Règle générale, les renseignements personnels sont accessibles uniquement aux personnes qui doivent y avoir accès dans l'exercice de leurs fonctions.

ARTICLE 2 - Champ d'application

Cette politique s'applique à l'égard des renseignements personnels que CAP santé mentale recueille, détient, utilise ou communique à des tiers, et ce, quelle que soit la nature du support et la forme sous laquelle les renseignements personnels sont détenus, à savoir écrite, graphique, sonore, visuelle, informatisée ou autre.

ARTICLE 3 - Définitions

3.1 **Employé :** toute personne qui travaille pour CAP santé mentale moyennant rémunération, incluant la direction générale, ainsi que toute personne non rémunérée (administrateur, bénévole, stagiaire).

3.2 **Participant :** tout individu qui fournit des renseignements personnels à CAP santé mentale en lien avec la réalisation d'un événement, la création d'une publication, la participation à une activité ou l'obtention d'un service.

3.3 **Événement, activité, service ou publication :**

3.3.1 Événement : toute activité que CAP santé mentale gère ou organise.

3.3.2 Activité : toute activité à laquelle un individu participe.

3.3.3 Service : tout service que CAP santé mentale rend à un individu à la demande de celui-ci.

3.3.4 Publication : toute publication produite par CAP santé mentale ou à laquelle elle contribue, sous quelque forme que ce soit, à savoir écrite, graphique, sonore, visuelle, informatisée ou autre.

3.4 **Renseignements personnels :** les renseignements personnels sont ceux qui portent sur une personne physique, recueillis sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) et qui permettent de l'identifier, y compris son nom, son numéro de téléphone, son adresse civique, son adresse de courrier électronique, le fait qu'elle ait été ou soit une participante à une activité ou ait demandé un service, son genre, son orientation sexuelle et toute information concernant sa santé. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée. Pour plus de certitude :

- les renseignements qui ne permettent pas d'identifier un individu dans le cadre d'un témoignage ne sont pas des renseignements personnels;

- les données statistiques ne sont pas des renseignements personnels puisqu'elles ne permettent pas d'identifier un individu;

- les photographies ou enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement personnel relatif à cet individu;

- les photographies ou enregistrements qui permettent d'identifier un individu comme EMPLOYÉ de CAP santé mentale ne constituent pas un renseignement personnel relatif à cet individu.

3.5 **Incident de confidentialité :** un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

3.6 **Risque sérieux de préjudice :** le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne responsable des renseignements personnels. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant la sensibilité des renseignements concernés, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.

3.7 **Registre des incidents de confidentialité :** l'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

3.8 **Formulaire de signalement :** le formulaire mis à la disposition de tout EMPLOYÉ ou PARTICIPANT servant à informer la personne responsable des renseignements personnels.

ARTICLE 4 - Obligation de confidentialité

Les EMPLOYÉS sont tenus de signer une entente de confidentialité (réf. : annexe 1) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de CAP santé mentale.

L'obligation de confidentialité s'applique à la durée de la relation d'un employé avec CAP santé mentale et survit à la fin de cette relation.

ARTICLE 5 - Collecte et usage des renseignements personnels

5.1 CAP santé mentale peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant les EMPLOYÉS. La constitution de tels dossiers a pour objet de :

- maintenir les coordonnées à jour;

- documenter des situations de travail ou de bénévolat;

- permettre, dans le cas des employés rémunérés, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurance collective, etc.).

5.2 CAP santé mentale peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant les PARTICIPANTS. La constitution de tels dossiers a pour objet de permettre à CAP santé mentale de réaliser une activité ou de fournir un service.

5.3 CAP santé mentale peut seulement recueillir les renseignements personnels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements personnels seulement à ces fins.

5.4 Les renseignements personnels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès d'autrui ou que la loi l'autorise.

ARTICLE 6 - Gestion des renseignements personnels

6.1 La direction générale, comme personne exerçant la plus haute autorité dans l'organisation, est la personne responsable d'assurer la protection des renseignements personnels. Elle peut déléguer cette responsabilité en la constatant par écrit (réf. : annexe 2). La direction générale ou la personne responsable s'assure de la tenue d'un registre des incidents de confidentialité.

6.2 La direction générale est autorisée à accéder à tout renseignement personnel que détient CAP santé mentale. Les autres employés sont autorisés à accéder aux renseignements personnels dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de leurs fonctions.

6.3 Lorsqu'un EMPLOYÉ ou un PARTICIPANT constate un incident de confidentialité, il doit informer avec diligence la direction générale ou la personne responsable de la protection des renseignements personnels afin qu'il soit inscrit au Registre. L'EMPLOYÉ ou le PARTICIPANT doit, pour ce faire, compléter un formulaire de signalement (réf. : annexe 3) et l'acheminer ensuite à la direction générale ou à la personne responsable.

Le Registre doit conserver les informations sur un incident de confidentialité pour une période de cinq ans. Doit être colligé dans le formulaire de signalement :

- une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description;

- une brève description des circonstances de l'incident;

- la date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue);

- la date ou la période à laquelle l'organisation s'est aperçue de l'incident;

- le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue).

6.5 La direction générale ou la personne responsable juge si l'incident présente un risque sérieux de préjudice. Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au Registre.

Si l'incident présente un risque sérieux de préjudice, la direction générale ou la personne responsable avise la Commission d'accès à l'information et les personnes concernées à l'aide du formulaire approprié (réf. : annexes 5 et 6).

Toutefois, le Règlement sur les incidents de confidentialité prévoit des situations où la communication peut se faire exceptionnellement par le biais d'un avis public, dont lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisme ou d'accroître le préjudice causé aux personnes concernées.

ARTICLE 7 - Conservation des renseignements personnels

7.1 Les EMPLOYÉS ayant accès aux dossiers en vertu de l'article 6.2 doivent :

- s'assurer que les renseignements personnels soient gardés à l'abri de tout dommage physique ou accès non autorisé;

- s'assurer que tous les documents électroniques comportant des renseignements confidentiels, incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. Ces mots de passe doivent être modifiés deux fois par année, ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées;

- garder les renseignements confidentiels en format papier dans des classeurs pouvant être verrouillés et s'assurer qu'ils soient verrouillés à la fin de chaque journée de travail. Les clés des classeurs doivent être gardées dans des endroits sûrs.

7.2 Un EMPLOYÉ peut également, à certains égards, être qualifié de PARTICIPANT. Si c'est le cas, les renseignements confidentiels concernant chaque titre sont conservés séparément.

7.3 Les dossiers constitués en vertu de cette politique sont la propriété de CAP santé mentale.

ARTICLE 8 - Destruction des renseignements personnels

8.1 Sous réserve de l'article 8.2, les renseignements personnels ne sont conservés que tant et aussi longtemps que l'objet pour lequel ils ont été recueillis n'a pas été accompli, à moins que l'individu concerné ait consenti à ce qu'il en soit autrement. Ces renseignements personnels sont ensuite détruits de façon à ce que les données y figurant ne puissent plus être reconstituées.

8.2 Les dossiers concernant les EMPLOYÉS sont conservés par CAP santé mentale.

8.3 Pour plus de certitude, les renseignements personnels concernant un individu ayant offert un témoignage, tels que son nom et ses coordonnées, sont détruits une fois le témoignage publié ou diffusé, à moins que l'individu ait préalablement consenti à ce que les renseignements personnels le concernant soient conservés pour permettre à CAP santé mentale de le recontacter dans le futur.

ARTICLE 9 - Divulgation de renseignements personnels à un tiers

9.1 Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article, les renseignements personnels ne peuvent être divulgués à un tiers qu'après l'obtention du consentement écrit, manifeste, libre et éclairé de la personne concernée. Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à sa réalisation.

9.2 Les renseignements personnels peuvent être divulgués sans le consentement de la personne concernée si la vie, la santé ou la sécurité de celle-ci est gravement menacée. La divulgation doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

9.3 Tel que permis par la loi, CAP santé mentale peut divulguer des renseignements personnels nécessaires à sa défense ou celle de ses EMPLOYÉS contre toute réclamation ou poursuite intentée contre elle ou ses EMPLOYÉS, par ou de la part d'un PARTICIPANT, d'un EMPLOYÉ, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un PARTICIPANT ou d'un EMPLOYÉ.

ARTICLE 10 - Communication de renseignements personnels à la personne concernée

10.1 Sous réserve de l'article 10.2, les PARTICIPANTS et EMPLOYÉS ont le droit de connaître les renseignements personnels que CAP santé mentale a reçus, recueillis et conserve à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

10.2 CAP santé mentale doit restreindre l'accès aux renseignements personnels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements personnels au sujet d'un tiers.

10.3 Une demande d'un PARTICIPANT ou d'un EMPLOYÉ en lien avec l'article 10.1 doit être traitée dans un délai maximal de 30 jours.

ARTICLE 11 - Manquement à l'obligation de confidentialité

11.1 Un EMPLOYÉ manque à son obligation de confidentialité lorsque cette personne :

- communique des renseignements personnels à des individus n'étant pas autorisés à y avoir accès;

- discute de renseignements personnels à l'intérieur ou à l'extérieur des locaux de CAP santé mentale alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de l'entendre;

- laisse des renseignements personnels sur papier ou support informatique à la vue dans un endroit où des individus n'étant pas autorisés à y avoir accès sont susceptibles de les voir;

- fait défaut de suivre les dispositions de cette politique.

11.2 Advenant un manquement à l'obligation de confidentialité, des mesures disciplinaires appropriées, pouvant aller jusqu'à la résiliation du contrat de travail ou de toute autre relation avec CAP santé mentale, seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées, au besoin, afin de s'assurer qu'un tel scénario ne se reproduise.

ARTICLE 12 - Recours

12.1 S'il s'avère que les renseignements personnels d'une personne ont été utilisés de façon contraire à une disposition de cette politique, cette personne peut déposer une plainte auprès de la direction générale de CAP santé mentale ou auprès du conseil d'administration de l'organisme si la plainte concerne la direction générale.

12.2 Lorsqu'un EMPLOYÉ ou un PARTICIPANT constate un incident de confidentialité, il doit communiquer avec la direction générale ou la personne responsable par le biais d'un formulaire de signalement prévu à cette fin (réf. : annexe 3). La direction générale ou la personne responsable :

- identifie les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents;

- évalue si l'incident présente un risque de préjudice sérieux, selon la grille d'analyse présentée à l'annexe 4;

- prévient sans délai la Commission d'accès à l'information via le formulaire prévu à cette fin (réf. : annexe 6) et toute personne dont les renseignements personnels sont affectés dans le cas où l'incident présente un risque de préjudice sérieux (réf. : annexe 5);

- tient un registre de tous les incidents;

- répond à la demande de la Commission d'accès à l'information d'avoir une copie du registre, le cas échéant.

12.3 Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements personnels la concernant peut déposer sa plainte auprès de la Commission d'accès à l'information pour l'examen du désaccord dans les 30 jours du refus de CAP santé mentale d'accéder à sa demande ou de l'expiration du délai pour y répondre.

ANNEXES

ANNEXE 1
Déclaration relative à la confidentialité

Je, soussigné·e, _____ déclare avoir lu la Politique et pratiques encadrant la gouvernance des renseignements personnels de CAP santé mentale et m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité survit à la fin de mon emploi, stage, bénévolat ou à ma fonction d'administrateur auprès de l'organisme.

Signé à Québec, le _____
date

Nom et prénom : _____
en lettres moulées

Signature : _____

ANNEXE 2

Formulaire de dérogation de la fonction de responsable de la protection des renseignements personnels

IDENTIFICATION de la plus haute autorité au sein de CAP santé mentale qui délègue tout ou en partie ses fonctions.

Nom et prénom : _____

Poste occupé au sein de l'organisme : _____

IDENTIFICATION de la personne responsable désignée.

Nom et prénom : _____

Poste occupé au sein de l'organisme : _____

RÔLES et RESPONSABILITÉS visés (cocher toutes les cases qui s'appliquent) :

- ❑ Toutes les responsabilités prévues par la Loi sur la protection des renseignements personnels dans le secteur privé.
- ❑ Établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels.
- ❑ Participer à la gestion des incidents de confidentialité.
- ❑ Tenir un registre des incidents de confidentialité.
- ❑ Sensibiliser le personnel, les partenaires et les tiers à la protection des renseignements personnels.

- ❑ Autre(s) :_____

PÉRIODE de délégation.

- ❑ Effectif du _____ au _____ .

- ❑ Effectif du _____ au _____ , et ce, jusqu'à la révocation par le délégant (en tout temps, le délégant peut retirer la présente délégation de responsabilités).

_____ _____

Signature du délégant Signature du délégataire

Date : Date :

ANNEXE 3
Formulaire de signalement

SECTION 1 - Date et période de l'incident de confidentialité

Date de l'incident : _____

Date de la découverte de l'incident : _____

L'incident a eu lieu sur une période de : _____

SECTION 2 - Type d'incident de confidentialité

- ❑ Accès non autorisé par la loi à un renseignement personnel.
- ❑ Utilisation non autorisée par la loi d'un renseignement personnel.
- ❑ Communication non autorisée par la loi d'un renseignement personnel.
- ❑ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

SECTION 3 - Causes et circonstances de l'incident (cochez toutes les cases qui s'appliquent)

- ❑ Altération délibérée
- ❑ Communication accidentelle
- ❑ Communication délibérée sans autorisation
- ❑ Consultation non autorisée
- ❑ Cyberattaque (virus, logiciel espion, etc.)
- ❑ Défaillance technique
- ❑ Destruction accidentelle
- ❑ Destruction volontaire sans autorisation
- ❑ Divulgation accidentelle
- ❑ Divulgation délibérée sans autorisation
- ❑ Erreur humaine
- ❑ Hameçonnage (phishing)
- ❑ Ingénierie sociale (technique de manipulation)
- ❑ Perte d'accès aux renseignements
- ❑ Perte de renseignements
- ❑ Rançongiciel
- ❑ Utilisation incompatible
- ❑ Vol de renseignements

❑ Autre, précisez : _____

SECTION 4 - Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident ?

- ❑ Ordinateur de bureau
- ❑ Dispositif amovible électronique
- ❑ Papier
- ❑ Clé USB
- ❑ Serveur
- ❑ CD
- ❑ Bande sonore
- ❑ Téléphone portable
- ❑ Infonuagique (cloud)
- ❑ Tablette
- ❑ Vidéosurveillance
- ❑ Ordinateur portable
- ❑ Photo

❑ Autre, précisez : _____

SECTION 5 - Identification des renseignements personnels visés par l'incident de confidentialité.

- ❑ Nom
- ❑ Prénom
- ❑ Adresse du domicile
- ❑ Date de naissance
- ❑ Numéro de téléphone au domicile
- ❑ Numéro du cellulaire
- ❑ Adresse courriel personnelle
- ❑ Numéro de permis de conduire
- ❑ Numéro d'assurance sociale
- ❑ Numéro d'assurance maladie
- ❑ Numéro de passeport
- ❑ Salaire / fonction / occupation
- ❑ Renseignements sur des employés
- ❑ Renseignements médicaux
- ❑ Renseignements génétiques
- ❑ Renseignements scolaires/académiques
- ❑ Renseignements bancaires
- ❑ Numéro de carte de crédit
- ❑ Numéro de carte de débit
- ❑ Numéro d'identification personnel (NIP)

❑ Autres renseignements personnels (précisez) :

_____

❑ Impossible de fournir une description des renseignements personnels visés (expliquez) :

_____

SECTION 6 - Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident : _____

Nombre de personnes concernées par l'incident qui résident hors Québec : _____

Lien avec l'organisme des personnes concernées par l'incident :

- ❑ Employé
- ❑ Bénévole
- ❑ Fournisseur
- ❑ Membre
- ❑ Participant à une activité

❑ Autre (précisez) : _____

SECTION 7 - Personne déclarant l'indicent

Prénom et nom : _____

Fonction : _____

Moyen de communication souhaité

- ❑ Courrier électronique : _____
- ❑ Téléphone : _____

ANNEXE 4
Grille d'analyse / Évaluation du « risque sérieux de préjudice »

Pour tout incident de confidentialité, CAP santé mentale doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

1. Quelle est la **sensibilité** des renseignements concernés.
2. Quelles sont les **conséquences appréhendées** de leur utilisation.
3. Quelle est la probabilité qu'ils soient utilisés à des **fins préjudiciables**.

1. Renseignements sensibles (sensibilité)

- Documents financiers.
- Dossiers médicaux.
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse), sauf si le contexte en fait des renseignements sensibles : nom, adresses associées à des périodiques spécialisés ou à des activités qui les identifient.

2. Préjudice grave (conséquences appréhendées)

- Humiliation.
- Dommage à la réputation ou aux relations.
- Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles.
- Perte financière.
- Vol d'identité.
- Effet négatif sur le dossier de crédit.
- Dommage aux biens ou leur perte.

3. Pour déterminer la probabilité d'un mauvais usage (fins préjudiciables)

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?
- Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
- Combien de temps les renseignements personnels ont-ils été exposés ?
- A-t-on constaté un mauvais usage des renseignements ?
- L'intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

Si l'analyse fait ressortir un préjudice sérieux, l'organisme avisera la Commission d'accès à l'information et les personnes concernées par l'incident. Dans le cas contraire, elle poursuivra tout de même ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau.

Le Commissariat à la protection de la vie privée du Canada a produit une vidéo d'aide à l'évaluation : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/atteinte_101/atteinte_risques/

ANNEXE 5

Avis de communication aux personnes concernées par un incident de confidentialité

MODÈLE

Dans le respect des obligations auxquelles elle est tenue en application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, CAP santé mentale souhaite vous informer de la survenance récente d'un incident de confidentialité qui concerne vos renseignements personnels.

[Insérer une description des renseignements personnels visés par l'incident (ex. : les renseignements personnels visés dans cet incident sont…) ou, si cette information n'est pas connue, la raison qui justifie l'impossibilité de les mentionner].

En effet, [insérer une brève description des circonstances de l'incident]. Cet incident est survenu [inscrire la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période].

Soyez [assurée/assuré] que CAP santé mentale met actuellement en œuvre des mesures afin de diminuer les risques qu'un préjudice vous soit causé. À cet égard, [inscrire une brève description des mesures que l'organisme a prises ou qu'il entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé].

De plus, afin d'optimiser la protection de vos renseignements personnels, nous vous suggérons [décrire les mesures que CAP santé mentale suggère à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer un tel préjudice].

Pour toute question ou précision complémentaire en lien avec cet incident en particulier, nous vous invitons à communiquer avec [inscrire les coordonnées qui permettront aux personnes concernées d'obtenir des informations supplémentaires relativement à l'incident].

ANNEXE 6

Avis à la commission d'accès à l'information
[document officiel prescrit par la CAI]

Commission d'accès à l'information du Québec

Section réservée à la Commission
Numéro de référence : _____
Date de réception : ___ / ___ / _____

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUX

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
Loi sur la protection des renseignements personnels dans le secteur privé

Objet du présent formulaire

Ce formulaire vise à permettre aux organisations[1] d'aviser la Commission d'accès à l'information (la Commission) de tout incident de confidentialité impliquant un renseignement personnel qu'elles détiennent et présentant un risque de préjudice sérieux.

On entend par « incident de confidentialité » :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Assurez-vous de ne pas transmettre de renseignements personnels permettant d'identifier une personne dans ce formulaire et dans tout autre document que vous transmettrez à la Commission.

Si vous manquez d'espace dans l'un des champs, joignez une annexe présentant l'ensemble de votre réponse lorsque vous transmettez le formulaire à la Commission et inscrivez « Voir annexe » dans le champ concerné.

Vous pouvez transmettre le formulaire et les documents joints par courrier électronique, par la poste ou par télécopieur aux coordonnées suivantes :

Commission d'accès à l'information
525, boulevard René-Lévesque Est, Bur. 2.36
Québec (Qc) G1R 5S9
Téléphone : 418 528-7741 – Sans frais : 1 888 528-7741 – Télécopieur : 418 529-3102
Courrier électronique : cai.communications@cai.gouv.qc.ca

[1] On entend par « organisation » : organisme public, personne qui exploite une entreprise, ordre professionnel, parti politique, député indépendant ou candidat indépendant, syndicat, association, organisme à buts non lucratifs, travailleur autonome et pigiste.

Commission d'accès à l'information du Québec

Obligations de l'organisation

- ✓ Évaluer si un incident de confidentialité représente un risque qu'un préjudice sérieux[2] soit causé aux personnes concernées par l'incident de confidentialité;
- ✓ Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent. Le fait de déclarer un incident de confidentialité à la Commission ne dispense pas une organisation de cette obligation;
- ✓ Aviser toute personne dont un renseignement personnel a été compromis par un incident de confidentialité si cet incident présente un risque qu'un préjudice sérieux soit causé. En cas de défaut, la Commission pourrait ordonner de le faire;
- ✓ Aviser la Commission, avec diligence, d'un incident de confidentialité impliquant un renseignement personnel qu'elle détient lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées;
- ✓ Transmettre à la Commission, dans les meilleurs délais, tout renseignement complémentaire dont elle prend connaissance après lui avoir transmis le présent avis;
- ✓ Inscrire l'incident déclaré dans son registre des incidents de confidentialité et communiquer ce dernier à la Commission sur demande.

Vous pouvez obtenir plus de renseignements au sujet de vos obligations en matière d'incident de confidentialité impliquant des renseignements personnels sur notre site Web à l'adresse https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/

Rôle de la Commission au regard des incidents de confidentialité

- La Commission s'assure que l'organisation respecte ses obligations légales lors d'un incident de confidentialité et qu'elle met en place les mesures nécessaires pour éviter que de nouveaux incidents de même nature ne se produisent.
- La Commission n'accompagne pas l'organisation dans la gestion des incidents de confidentialité.
- La Commission ne procède pas à la validation des mesures prises par l'organisation pour diminuer les risques qu'un préjudice soit causé ou pour éviter que de nouveaux incidents de même nature se produisent.
- Le fait d'aviser la Commission d'un incident de confidentialité ne peut servir à établir la conformité des pratiques d'une organisation à l'égard de ses obligations légales.

[2] Le préjudice sérieux n'a pas à s'être matérialisé. Il peut seulement être susceptible de se produire.

Commission d'accès à l'information du Québec

1. Identification de l'organisation concernée par l'incident de confidentialité
(Veuillez remplir la section A pour un organisme public et la section B pour une entreprise)

A. Identification de l'organisme public

Nom :	
Adresse :	
Personne à contacter relativement à l'incident	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

B. Identification de l'entreprise

Nom :	
Adresse du siège social :	
Numéro d'entreprise au Québec (selon le Registraire du Québec) :	
Dirigeant principal	
Nom :	Titre / fonction :
Téléphone :	Courriel :
Personne à contacter relativement à l'incident ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

Commission d'accès à l'information du Québec

2. Date et période de l'incident de confidentialité

Date de l'incident :	Date de découverte de l'incident :
L'incident a eu lieu sur une période de :	

3. Type d'incident de confidentialité

- ☐ Accès non autorisé par la loi à un renseignement personnel
- ☐ Utilisation non autorisée par la loi d'un renseignement personnel
- ☐ Communication non autorisée par la loi d'un renseignement personnel
- ☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

3.1 Causes et circonstances de l'incident de confidentialité

Selon le type d'incident sélectionné ci-dessus, identifiez la ou les cause(s) de celui-ci :

☐ Altération délibérée	☐ Communication accidentelle	☐ Communication délibérée sans autorisation	☐ Consultation non autorisée
☐ Cyberattaque (virus, logiciel espion, etc.)	☐ Défaillance technique	☐ Destruction accidentelle	☐ Destruction volontaire sans autorisation
☐ Divulgation accidentelle	☐ Divulgation délibérée sans autorisation	☐ Erreur humaine	☐ Hameçonnage (phishing)
☐ Ingénierie sociale	☐ Perte d'accès aux renseignements	☐ Perte de renseignements	☐ Rançongiciel
☐ Utilisation incompatible	☐ Vol de renseignements	☐ Autre Précisez :	

Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :

Commission d'accès à l'information du Québec

Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident :	
☐ Ordinateur de bureau	☐ Dispositif amovible électronique
☐ Papier	☐ Clé USB
☐ Serveur	☐ CD
☐ Bande sonore	☐ Téléphone portable
☐ Infonuagique (cloud)	☐ Tablette
☐ Vidéosurveillance	☐ Ordinateur portable
☐ Photo	☐ Autre Précisez :

4. Description des renseignements personnels visés par l'incident de confidentialité

☐ Nom ☐ Prénom	☐ Adresse du domicile	☐ Date de naissance ou ☐ Année ☐ Mois ☐ Jour ☐ Âge
☐ Numéro de téléphone au domicile	☐ Numéro du cellulaire	☐ Adresse courriel personnelle

☐ Numéro de permis de conduire	☐ Numéro d'assurance sociale
☐ Numéro d'assurance maladie	☐ Numéro de passeport
☐ Salaire	☐ Fonction / occupation

☐ Renseignements sur des employés, clients ou bénéficiaires
Précisez :

☐ Renseignements médicaux
Précisez :

☐ Renseignements génétiques
Précisez :

☐ Renseignements scolaires / académiques
Précisez :

☐ Renseignements bancaires / numéro de compte / institution / placements / hypothèque
Précisez :

☐ Numéro de carte de crédit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	☐ Code de sécurité à trois chiffres
☐ Numéro de carte de débit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	

☐ Autres renseignements personnels

Précisez :

☐ Impossible de fournir une description des renseignements personnels visés

Expliquez :

5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

6. Évaluation par l'organisation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.

Commission d'accès à l'information du Québec

Décrivez les raisons qui supportent l'existence d'un risque de préjudice sérieux pour les personnes concernées par l'incident.

Le responsable de la protection des renseignements personnels de votre organisation a-t-il été consulté pour procéder à l'évaluation du risque de préjudice?

◯ Oui ◯ Non

7. Avis de l'organisation aux personnes concernées
(Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)

L'organisation a-t-elle avisé les personnes concernées par l'incident de confidentialité?

◯ Non
◯ Oui. L'avis a été fait par :

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par l'organisation afin de le faire?

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis prévu :

☐ Aucune notification de l'incident aux personnes concernées n'est prévue.
Expliquez :

Commission d'accès à l'information du Québec

7.1 Contenu de l'avis aux personnes concernées

Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par l'organisation.

- ☐ Une description des renseignements personnels visés par l'incident
- ☐ Une brève description des circonstances de l'incident
- ☐ La date ou la période où l'incident a eu lieu
- ☐ Une brève description des mesures que l'organisation a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
- ☐ Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice
- ☐ Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par l'organisation?

- ◯ Non.
- ◯ Oui. Combien :

  Expliquez :

7.2 Avis public aux personne concernées

L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?

- ◯ Non
- ◯ Oui. Sélectionnez la raison applicable :

  - ☐ Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.

    Expliquez :
  - ☐ Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour l'organisation.

    Expliquez :
  - ☐ L'organisation n'a pas les coordonnées des personnes concernées.

    Expliquez :

Commission d'accès à l'information du Québec

Par quels moyens l'avis public a-t-il été fait?
☐ Un avis dans les médias Précisez lesquels : Date de diffusion :
☐ Un communiqué de presse Date de diffusion :
☐ Un avis sur le site Web de l'organisation
☐ Une conférence de presse Lieu : Date :
☐ Une publication diffusée dans les médias sociaux Précisez lesquels :
☐ Autre Précisez :
Est-ce que l'organisation a avisé d'autres autorités de protection des renseignements personnels à l'extérieur du Québec?
☐ Commissaire à la protection de la vie privée du Canada
☐ Office of the information and privacy commissioner of Alberta
☐ Office of the information and privacy commissioner of British Columbia
☐ Commissaire à l'information et à la protection de la vie privée de l'Ontario
☐ Autre. Précisez :

Commission d'accès à l'information du Québec

8. Obligation de diminuer le risque de préjudice

Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées?

Dans quel délai ces mesures ont-elles été prises?

Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent?

- ◯ Non
- ◯ Oui. Précisez :

Y a-t-il des mesures prévues qui n'ont pas encore été prises?

- ◯ Non
- ◯ Oui. Précisez :

Indiquez la date de mise en place des mesures prévues :

Une organisation doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.

Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté?

- ◯ Non
- ◯ Oui. Précisez lesquelles et indiquez l'échéancier prévu :

Commission d'accès à l'information du Québec

9. Signature

Prénom :	Nom :
Fonction :	Lieu / Ville :
Date de transmission du formulaire à la Commission :	
Pour le compte de : ◯ l'organisme ◯ l'entreprise	
Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.	
Signature :	