Procédures relatives à la gestion des cas d'atteinte à la vie privée

La Société canadienne de la SP (« Société de la SP ») s'est engagée à respecter la vie privée des personnes qui vivent avec la SP, de ses membres, des participants à ses événements, de ses donateurs, de ses bénévoles et de ses employés et à protéger les renseignements personnels qu'elle recueille, utilise, divulgue et conserve.

Bien que la protection de l'information soit de la plus haute importance pour la Société de la SP (comme elle le souligne dans sa Politique de protection de la vie privée et de la confidentialité et les procédures s'y rattachant), nous savons qu'elle n'est pas à l'abri des atteintes à la vie privée. C'est pourquoi elle décrit dans le présent document la marche à suivre par ses employés et ses bénévoles dans les cas d'atteinte à la vie privée.

Qu'est-ce qu'une atteinte à la vie privée?

Une atteinte à la vie privée suppose l'accès non autorisé à des renseignements personnels ou à de l'information sur la santé détenus par la Société de la SP sur les participants à ses programmes et événements, les prestataires de ses services, ses donateurs, ses employés et ses bénévoles, ou la collecte, l'utilisation ou la communication non autorisées de tels renseignements. Ces activités sont « non autorisées » lorsqu'elles contreviennent à notre Politique de protection de la vie privée et de la confidentialité (qui se conforme à la Loi sur la protection des renseignements personnels et les documents électroniques [LPRPDE] et sur les lois provinciales pertinentes).

Certains des cas d'atteinte à la vie privée les plus fréquents se produisent lorsque des renseignements personnels détenus par la Société de la SP sont volés, perdus ou communiqués par erreur. Ces atteintes peuvent survenir lorsqu'un ordinateur contenant des renseignements personnels ou de l'information sur la santé est volé ou lorsque des courriels contenant des renseignements personnels sont envoyés par erreur aux mauvais destinataires ou encore lorsque les noms et les coordonnées de nos donateurs sont transmis à un autre organisme sans l'accord de ces derniers.

OBJECTIFS

Le présent document se veut un guide à l'intention des employés et des bénévoles dans la gestion des cas d'atteinte à la vie privée. Il décrit la marche à suivre pour s'assurer d'abord qu'il y a bien eu atteinte à la vie privée et, le cas échéant, pour limiter les conséquences de l'atteinte, aviser les personnes concernées, documenter

l'incident, faire enquête et apporter les changements nécessaires pour éviter que cela ne se reproduise.

APPROBATION

Les présentes procédures ont été approuvées par l'équipe de la haute direction, le 28 octobre 2015.

PROCÉDURES

La Société de la SP vérifie toutes les plaintes relatives à une atteinte à la vie privée. Si l'atteinte portée à sa connaissance est confirmée, la Société de la SP évalue la situation et prend rapidement les mesures nécessaires.

Tout employé ou tout bénévole qui prend conscience d'un cas d'atteinte à la vie privée, voire de la possibilité d'un tel incident, doit prendre immédiatement les mesures énumérées plus bas.

La Société de la SP assure la protection de tout employé ou bénévole qui signale un cas possible d'atteinte à la vie privée ou de non-respect de la Politique de protection de la vie privée et de la confidentialité de la Société de la SP ou de la législation pertinente. (Pour obtenir tous les détails à ce sujet, consultez la Politique relative au signalement d'actes répréhensibles, commis par des employés ou des bénévoles en position de leadership, et à la protection des divulgateurs). Cette protection est étendue aux personnes qui refusent d'accomplir une tâche qui, selon elles, contrevient aux lois applicables ou à la Politique de protection de la vie privée et de la confidentialité de la Société de la SP.

Voici les cinq étapes de la gestion d'une atteinte à la vie privée :

1. Rapporter l'atteinte, réelle ou soupçonnée.
2. Limiter l'atteinte.
3. Évaluer les risques associés à l'atteinte.
4. Aviser les personnes concernées.
5. Documenter l'atteinte, faire enquête et apporter les mesures correctives nécessaires.

1re ÉTAPE : Rapporter l'atteinte, réelle ou soupçonnée

1.1 Rapporter une atteinte possible à la vie privée

Toute personne travaillant au nom de la Société de la SP qui prend conscience d'une atteinte à la vie privée découlant de la divulgation de renseignements personnels ou d'information sur la santé sous la garde ou le contrôle de la Société de la SP ou qui soupçonne la survenue d'une telle atteinte doit en aviser immédiatement son supérieur, la personne responsable de la protection de la vie privée de sa division et

celle du Bureau national. (Vous trouverez les coordonnées de ces personnes à **l'annexe B**.)

En présence d'un possible conflit d'intérêts ou pour tout autre motif, par souci de confidentialité et conformément à notre Politique relative au signalement d'actes répréhensibles commis par des employés ou des bénévoles en position de leadership et à la protection des divulgateurs ainsi qu'aux procédures s'y rattachant, ce type d'allégations peut être adressé à l'une des personnes suivantes :

- directeur général de la division concernée;
- président et chef de la direction de la Société de la SP;
- préposé au service d'assistance téléphonique externe pour le signalement d'actes répréhensibles : 1 866 921-6714.

Le signalement d'une atteinte à la vie privée doit comporter les réponses aux questions suivantes :

- Que s'est-il passé?
- Dans quel service?
- À quelle date?
- Comment et quand l'incident a-t-il été découvert?
- Quel type de données sont en cause et combien de personnes sont concernées?
- Des correctifs ont-ils déjà été apportés?

La personne responsable de la protection de la vie privée (PRPVP) de la division concernée informera son homologue au Bureau national ainsi que le directeur général de sa division de la survenue possible d'une atteinte à la vie privée et elle se penchera sur les circonstances entourant l'événement. Cet incident sera documenté et consigné dans une base de données sur les atteintes à la vie privée.

1.2 Évaluer le fondement de la plainte

La PRPVP de la division déterminera, en collaboration avec son homologue du Bureau national, s'il s'agit bien d'une atteinte à la vie privée.

Pour évaluer le fondement d'une plainte relative à une atteinte à la vie privée, il faut se poser les deux questions fondamentales suivantes :

1. **Des renseignements personnels ont-ils été divulgués?** Déterminer le type de renseignements en cause pour confirmer qu'il y a bel et bien atteinte à la vie privée. Les renseignements personnels sont des renseignements détenus sur des personnes identifiables, portant par exemple sur la race, la nationalité, la religion, l'âge, le statut matrimonial, le niveau d'instruction, l'état de santé (révélant par exemple un diagnostic de SP), des données financières, l'adresse, le numéro de téléphone, des opinions personnelles, etc.
2. **Une divulgation non autorisée de renseignements est-elle survenue?** Qu'elle ait été intentionnelle ou accidentelle ou qu'elle découle d'une activité

criminelle, la divulgation non autorisée de renseignements personnels constitue une atteinte à la vie privée.

Si les réponses à ces deux questions sont affirmatives, il y a bel et bien eu atteinte à la vie privée. La PRPVP de la division doit alors passer aux étapes suivantes de la marche à suivre décrites ci-dessous.

1.3 Intervenir relativement aux cas d'atteinte à la vie privée

Dès qu'une atteinte à la vie privée est confirmée, la PRPVP de la division en informera les personnes suivantes :

- la personne ayant signalé l'atteinte ou la possibilité d'une atteinte à la vie privée;
- la personne responsable de la protection de la vie privée du Bureau national;
- le vice-président adjoint du marketing et des communications;
- le vice-président des technologies de l'information;
- le directeur général de la division (dans les cas d'incidents de portée régionale);
- le président et chef de la direction de la Société de la SP (dans les cas d'incidents de portée nationale);
- le vice-président en chef des finances (qui informera l'assureur de la Société de la SP de la situation).

La PRPVP du Bureau national informera aussi les membres de l'équipe de la haute direction de la situation et tiendra ces derniers au courant de l'évolution de la situation.

La confirmation d'une atteinte à la vie privée doit être obtenue dans les 24 heures suivant le premier signalement.

1.4 Former une équipe d'intervention

Aussitôt qu'une atteinte à la vie privée est confirmée, la PRPVP du Bureau national formera une équipe chargée d'intervenir dès qu'il sera raisonnablement possible de le faire, et elle dirigera la mise en œuvre des dernières étapes de la marche à suivre prévue en cas d'atteinte à la vie privée.

Outre les PRPVP du Bureau national et de la division concernée, l'équipe d'intervention peut comprendre un responsable de la sécurité de l'information, la personne ayant signalé l'incident, un représentant du Service du marketing et des communications, un membre de l'équipe de la haute direction et d'autres membres concernés. Certains employés peuvent être appelés à assister cette équipe dans son mandat.

Les noms et les coordonnées des PRPVP et d'autres personnes clés sont fournis à **l'annexe B**.

2e ÉTAPE : Limiter l'atteinte

Dès la survenue d'une atteinte à la vie privée, les mesures suivantes doivent être prises. Certaines d'entre elles peuvent être mises en œuvre simultanément (p. ex. la notification et la limitation de l'atteinte).

Avec l'aide de la PRPVP de la division et d'autres personnes concernées, la personne ayant découvert l'atteinte à la vie privée prendra immédiatement des mesures afin de limiter l'atteinte en prévenant toute future diffusion non autorisée de l'information en cause (p. ex. en mettant fin à la pratique non autorisée, en récupérant les données, en éteignant le système qui fait l'objet de la brèche, en révoquant ou en changeant les codes d'accès informatiques, en corrigeant les lacunes des systèmes de sécurité, etc.). Les mesures de limitation de l'atteinte à la vie privée doivent être prises en même temps que l'envoi de l'avis pertinent (p. ex. si une télécopie a été envoyée à un mauvais numéro de téléphone, communiquez avec la personne à qui appartient ce numéro et demandez-lui de ne pas lire la télécopie reçue, de la déchiqueter et de vous envoyer un courriel confirmant qu'elle a accédé à votre demande). Les mesures de limitation de l'atteinte comprennent les suivantes :

- Récupérer le plus grand nombre de données divulguées possible (idéalement toutes).
- Détruire toutes les copies des données collectées sans autorisation.
- S'assurer qu'aucune copie des renseignements confidentiels en cause n'a été produite ou conservée par la personne dont l'accès à ces renseignements était interdit; obtenir les coordonnées de cette personne au cas où un suivi serait nécessaire.
- Faire en sorte qu'aucune autre atteinte à la vie privée ne puisse être réalisée de la même façon.

L'équipe d'intervention en cas d'atteinte à la vie privée s'emploiera à déterminer si l'atteinte à la vie privée signalée pourrait permettre l'accès non autorisé à d'autres renseignements personnels ou information personnelle sur la santé (p. ex. un système d'information électronique) et à prendre les dispositions qui s'imposent (p. ex. changer les mots de passe et les codes d'utilisateurs et éteindre temporairement un système).

En consultation avec le conseiller juridique et le président et chef de la direction de la Société de la SP, la PRPVP du Bureau national communiquera avec la police si l'atteinte découle ou semble découler d'une activité criminelle.

Consultez l'**annexe A** pour avoir un aperçu du processus de notification d'une atteinte à la vie privée.

3e ÉTAPE : Évaluer les risques associés à l'atteinte

Pour connaître les autres étapes à franchir dans l'immédiat, l'équipe d'intervention en cas d'atteinte à la vie privée évaluera les risques associés à l'atteinte en question en prenant les facteurs suivants en considération :

- **La nature des renseignements personnels en cause**
  - Quels éléments d'information sont en cause dans l'atteinte à la vie privée? En général, plus les renseignements sont sensibles, plus les risques sont grands. L'information sur l'état de santé et les données sur la situation financière sont de bons exemples de renseignements sensibles qui pourraient être utilisés par un usurpateur d'identité.
  - Quelle utilisation pourrait être faite de l'information personnelle? Cette information pourrait-elle être utilisée à des fins frauduleuses ou autrement préjudiciables?

- **La cause et l'étendue de l'atteinte à la vie privée**
  - Quelle est la cause de l'atteinte en question?
  - Les renseignements personnels risquent-ils de demeurer exposés ou de faire l'objet d'une exposition accrue?
  - Quelle est l'étendue de la collecte, de l'utilisation ou de la divulgation non autorisées des données? Combien de personnes ont pu recevoir ces renseignements, et quels sont les risques liés à l'accès, l'utilisation ou la divulgation futurs de ces données, y compris par les médias de masse ou en ligne?
  - L'information est-elle cryptée ou autrement inaccessible rapidement?
  - Quelles mesures ont déjà été prises pour réduire les risques de préjudice au minimum?

- **Les personnes touchées par l'atteinte à la vie privée**
  - Combien de personnes sont touchées par cette atteinte?
  - Qui sont ces personnes : des participants aux programmes et aux événements de la Société de la SP, des prestataires de services offerts par la Société de la SP, des donateurs, des bénévoles, des employés, des fournisseurs de services, d'autres organismes?

- **Préjudices prévisibles découlant de l'atteinte à la vie privée**
  - Y a-t-il une relation entre les destinataires non autorisés des renseignements en cause et la nature de ces renseignements?
  - À quel genre de préjudice pourraient être exposées les personnes touchées par cette atteinte à la vie privée? Il pourrait s'agir de risques liés à la sécurité (p. ex. sécurité physique), de vol d'identité ou de fraude, de perte d'occasions d'affaires ou de possibilités d'emploi et de souffrance, d'humiliation, d'atteinte à la réputation ou de détérioration des relations.

- Quel genre de préjudice cette atteinte à la vie privée pourrait-elle causer à la Société de la SP? (Citons par exemple la perte de confiance envers la Société de la SP, la perte d'actifs et des risques financiers).

Si on juge que le risque nuira considérablement à la réputation de la Société de la SP, le vice-président adjoint du marketing et des communications ou d'autres personnes clés envisageront de mettre en œuvre le plan de communication en situation de crise. Si le risque pour la sécurité de nos technologies de l'information (TI) est modéré ou élevé, le vice-président des TI envisagera de mettre en œuvre le plan de reprise informatique après catastrophe.

4e ÉTAPE : Aviser les personnes ou les établissements concernés

Le processus de notification dépend de la nature de l'atteinte. L'équipe d'intervention en cas d'atteinte à la vie privée jugera de la nécessité d'aviser les personnes et les établissements concernés en se fondant sur les lignes directrices suivantes :

4.1 Comment savoir s'il faut aviser les personnes ou les établissements concernés d'une atteinte à leur vie privée

Les points suivants vous aideront à prendre une décision quant à la pertinence d'informer les personnes concernées d'une atteinte à leur vie privée. Si l'un des deux premiers facteurs énoncés ci-dessous s'applique, les personnes concernées doivent être informées de la situation. La liste des facteurs de risque suivants se veut un guide. Si aucun de ces facteurs ne s'applique à la situation, aucune notification n'est nécessaire. L'équipe d'intervention en cas d'atteinte à la vie privée doit faire preuve de jugement dans l'évaluation de la nécessité d'aviser les personnes concernées.

Points à considérer :

1. ***La loi exige que les personnes concernées soient informées de la situation.***
2. ***Un avis doit être transmis en vertu des dispositions d'un contrat.***
3. ***Il y a risque de vol d'identité.***
    - Le vol d'identité est inquiétant lorsque des renseignements volés ne sont pas cryptés, tels des noms liés à des numéros de carte de crédit ou d'assurance maladie ou toute autre information qui pourrait être utile à des fraudeurs.
4. ***Il y a risque de préjudice physique.***
    - La perte des données en cause risque-t-elle d'entraîner des préjudices physiques ou une forme ou une autre de harcèlement?
5. ***Il y a risque de souffrance, d'humiliation, d'atteinte à la réputation.***

- La perte des données en cause risque-t-elle d'entraîner de la souffrance ou de l'humiliation pour les personnes concernées ou une atteinte à leur réputation? Ce type de préjudice est à craindre surtout lorsque l'information divulguée porte sur le dossier médical des personnes concernées.

6. Il y a risque de perte d'occasions d'affaires ou de possibilités d'emploi

- La perte des données en cause pourrait-elle entraîner une atteinte à la réputation de la personne concernée ou le risque de perdre des occasions d'affaires ou des possibilités d'emploi?

Les personnes concernées doivent être informées de la survenue d'une atteinte à leur vie privée dès qu'il est raisonnablement possible de le faire. Toutefois, si le dossier est entre les mains de la police, il se peut que les autorités policières vous demandent de retarder la communication de cette information afin de ne pas nuire à une éventuelle enquête criminelle.

4.2 Méthode de notification

La méthode de notification privilégiée consiste à communiquer directement – par téléphone, par écrit ou en personne – avec les personnes concernées. Les facteurs suivants militent en faveur d'une **notification directe** :

- L'identité des personnes concernées est connue.
- Les coordonnées actuelles des personnes concernées sont disponibles.
- Les personnes concernées demandent des détails sur l'atteinte à leur vie privée afin de pouvoir se protéger elles-mêmes contre tout préjudice qui pourrait en découler.
- Les personnes concernées peuvent avoir de la difficulté à comprendre une notification indirecte (en raison de leur état mental, de leur âge, de la langue utilisée, etc.).

La notification indirecte – affichage d'avis, diffusion de l'information sur le site Web ou par l'entremise d'annonces ou de communiqués de presse – devrait généralement être réservée aux situations où la notification directe pourrait aggraver le préjudice subi par les personnes concernées ou augmenter le coût de la démarche et où les coordonnées des personnes concernées ne sont pas disponibles. Dans certains cas, la méthode la plus efficace consiste à recourir à plusieurs méthodes de notification. Les facteurs suivants militent en faveur d'une **notification indirecte** :

- Un très grand nombre de personnes sont concernées par l'atteinte à la vie privée en question, de sorte qu'une notification directe pourrait s'avérer impossible.
- Une notification directe pourrait aggraver le préjudice subi par les personnes concernées.

4.3 Information à transmettre lors de la notification aux personnes concernées

L'équipe d'intervention en cas d'atteinte à la vie privée rédigera la notification et désignera les signataires.

Cette notification a pour but de fournir les renseignements suivants aux personnes concernées :

- Ce qui s'est passé et la date de l'atteinte.
- Une description générique du ou des types de renseignements personnels divulgués, y compris les données personnelles nominatives.
- La nature des risques réels ou potentiels de préjudices.
- Les mesures d'intervention déjà prises par la Société de la SP.
- Les mesures que devraient prendre les personnes concernées pour se protéger contre les préjudices potentiels (p. ex. le suivi des comptes de crédit, la surveillance des comptes bancaires, les manières de communiquer avec les agences d'évaluation du crédit, etc.).
- Les correctifs prévus par la Société de la SP pour éviter d'autres atteintes à la vie privée.
- Les coordonnées de la personne avec laquelle communiquer à la Société de la SP pour obtenir de plus amples renseignements.

5e ÉTAPE : Documenter l'atteinte, faire enquête et apporter les mesures correctives nécessaires

5.1 Documenter l'atteinte

Tous les détails relatifs à une atteinte à la vie privée, qu'elle soit réelle ou potentielle, doivent être documentés, de même que les mesures correctives qui ont été apportées. Ces incidents doivent être consignés dans la base de données sur les atteintes à la vie privée, qui est accessible dans *mercure*, sur le site de l'équipe d'intervention en cas d'atteinte à la vie privée.

Les renseignements suivants seront consignés par l'équipe d'intervention en cas d'atteinte à la vie privée :

- La nature et la portée de l'atteinte (p. ex. le nombre de personnes touchées, le type de renseignements personnels en cause, la mesure dans laquelle l'atteinte a été limitée), mais si cette information n'est pas connue au moment de l'entrée des données, il faudra l'indiquer.
- La stratégie de gestion de l'atteinte à la vie privée qui a été mise en place ou prévue.
- Le plan de notification des personnes concernées ou d'autres personnes, s'il y a lieu.
- Si le signalement de l'atteinte provient de l'extérieur (p. ex. d'une personne, d'un autre organisme ou d'un fournisseur de services externe), les renseignements suivants doivent être recueillis : information fournie lors du

signalement, coordonnées du divulgateur au cas où un suivi serait nécessaire, et toutes les instructions données au divulgateur (p. ex. retourner les documents envoyés à la mauvaise adresse).
- Le calendrier des points d'information réguliers adressés à l'équipe de la haute direction sur l'atteinte en question et la gestion de la situation.

5.2 Enquête et mesures correctives

La PRPVP du Bureau national, en collaboration avec l'équipe d'intervention en cas d'atteinte à la vie privée, mènera une enquête interne visant à :

- cerner et à analyser les événements qui ont mené à la découverte de l'atteinte à la vie privée en question;
- évaluer ce qui a été fait pour limiter l'atteinte;
- recommander des moyens de prévenir d'autres atteintes à la vie privée, entre autres :
  - revoir les processus internes pertinents afin de s'assurer qu'ils sont conformes à notre Politique de protection de la vie privée et de la confidentialité;
  - modifier ou renforcer les politiques et pratiques courantes de gestion et de protection des renseignements personnels;
  - élaborer de nouvelles mesures de sécurité et de protection de la vie privée et les mettre en œuvre;
  - informer le personnel sur les exigences des lois pertinentes, les politiques, les pratiques et les procédures en matière de sécurité et de protection de la vie privée;
  - tester les mesures correctives et les évaluer afin de déterminer si elles ont été bien mises en œuvre et si les politiques et les pratiques doivent être modifiées.

SURVEILLANCE ET CONFORMITÉ

Les personnes responsables de la protection de la vie privée à tous les échelons de la Société de la SP doivent s'assurer de la conformité à ces procédures.

Tous les cas confirmés d'atteinte à la vie privée doivent être mentionnés dans le rapport trimestriel sur la conformité à la politique et aux procédures pertinentes, soumis au président et chef de la direction de la Société de la SP par les membres de l'équipe de la haute direction.

POLITIQUES, LOIS ET DOCUMENTS RÉFÉRENTIELS PERTINENTS

- Politique de protection de la vie privée et de la confidentialité de la Société de la SP
- Société canadienne de la SP – La vie privée et vous – Guide de mise en œuvre de la politique de protection de la vie privée et de la confidentialité

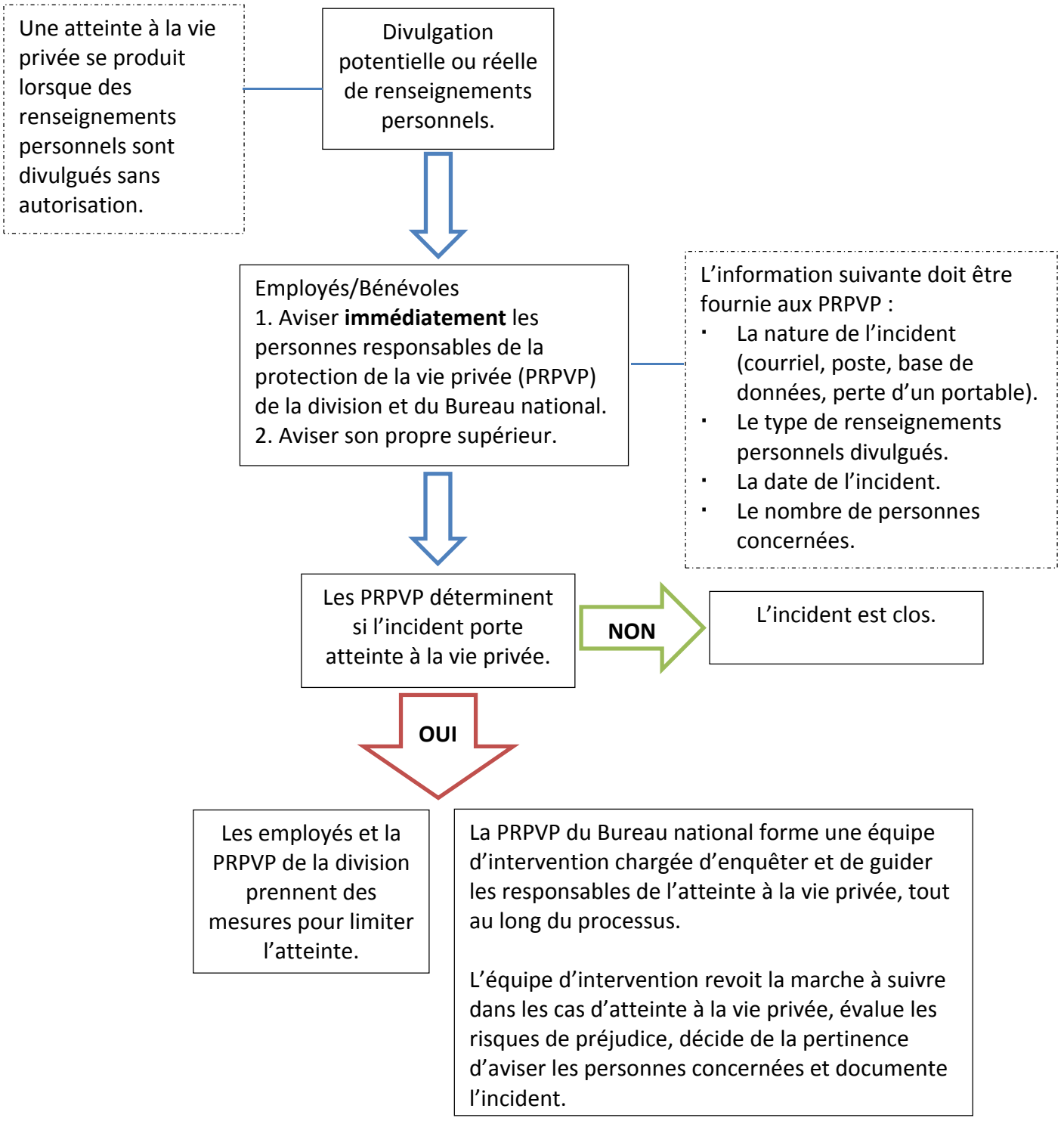
- Politique relative au signalement d'actes répréhensibles, commis par des employés ou des bénévoles en position de leadership, et à la protection des divulgateurs
- Guide de mise en œuvre de la Politique relative au signalement d'actes répréhensibles, commis par des employés ou des bénévoles en position de leadership, et à la protection des divulgateurs

REVUE DES PROCÉDURES

Les présentes procédures ainsi que la Politique de protection de la vie privée et de la confidentialité à laquelle elles se rattachent doivent être passées en revue tous les cinq ans.

Annexe A

PROCESSUS DE NOTIFICATION D'UNE ATTEINTE À LA VIE PRIVÉE



Annexe B

COORDONNÉES DES PERSONNES RESPONSABLES DE LA PROTECTION DE LA VIE PRIVÉE

Adresses électroniques des **personnes responsables de la protection de la vie privée** :

Responsable de la protection de la vie privée du Bureau national	Adresse française : priv@scleroseenplaques.ca Adresse anglaise : priv@mssociety.ca
Responsables de la protection de la vie privée des divisions	
Alberta et T.N.-O.	priv-alberta@mssociety.ca
Atlantique	priv-atlantic@mssociety.ca
Colombie-Britannique et Yukon	priv-bc@mssociety.ca
Manitoba	priv-manitoba@mssociety.ca
Ontario et Nunavut	priv-ontario@mssociety.ca
Québec	priv-quebec@scleroseenplaques.ca
Saskatchewan	priv-sask@mssociety.ca

Les noms et les coordonnées des PRPVP peuvent changer de temps à autre. Cliquez ici pour accéder au site d'équipe commun de la protection de la vie privée, où vous trouverez l'information courante.

Autres personnes clés à aviser en cas d'atteinte à la vie privée :

Vice-président adjoint du marketing et des communications

Vice-président des technologies de l'information

Président ou directeur général de la division concernée (dans les cas d'incidents à portée régionale)

Président et chef de la direction de la Société de la SP (dans les cas d'incidents à portée nationale)

Vice-président en chef des finances

Annexe C

ÉLÉMENTS À CONSIGNER EN CAS D'ATTEINTE À LA VIE PRIVÉE

Date du signalement	
Date et heure de la découverte de l'atteinte	

A. Coordonnées

Nom du divulgateur de l'atteinte (réelle ou potentielle)	
Titre et coordonnées de cette personne	
Nom de son superviseur (s'il y a lieu)	

B. Description de l'incident

Décrire la nature et la cause de l'atteinte à la vie privée. Quand et comment fut-elle découverte? Où est-elle survenue?

C. Limitation de l'atteinte et évaluation de ses risques

Répondre à chacune des questions suivantes, puis, à partir des réponses fournies, évaluer sommairement les risques encourus.

(1) Limitation de l'atteinte

Cocher tous les facteurs qui s'appliquent :

	Les renseignements personnels divulgués ont été récupérés, et toutes les copies sont actuellement sous notre garde et notre contrôle.
	Nous avons la confirmation que les renseignements en cause n'ont pas été copiés.
	Nous avons la confirmation que les renseignements personnels en cause ont été détruits.

	Nous croyons (sans toutefois en avoir reçu la confirmation) que les renseignements personnels en cause ont été détruits.
	Les renseignements personnels en cause étaient cryptés.
	Les renseignements personnels en cause n'étaient pas cryptés.
	Les données réunies jusqu'ici portent à croire que l'incident provient d'un problème systémique.
	Les données réunies jusqu'ici portent à croire qu'il s'agit probablement d'un incident isolé.
	Les renseignements personnels en cause n'ont pas été récupérés, mais des mesures visant à limiter l'atteinte ont été mises en place (cocher tout ce qui s'applique ci-dessous) :
	l'environnement immédiat de la source de l'atteinte à la vie privée a été fouillé minutieusement;
	le service des TI a été avisé;
	tous les mots de passe et les noms des utilisateurs du système ont été modifiés.
Décrire toute autre méthode employée pour limiter l'atteinte :	

(2) Nature des renseignements personnels en cause

Lister tous les éléments d'information divulgués (p. ex. nom, date de naissance, adresse courriel, adresse postale, maladies diagnostiquées, lien avec un fournisseur de soins tel un psychologue, etc.).

	Nom
	Adresse courriel
	Adresse postale
	Date de naissance
	Données financières
	Information sur les donateurs
	Renseignements médicaux (p. ex. diagnostic de SP)
	Caractéristiques personnelles comme la race, la religion, l'orientation sexuelle
	Autre (veuillez préciser)

(3) Liens

Quel est le lien entre le destinataire non autorisé des renseignements personnels et les personnes concernées par l'atteinte à la vie privée?

	Aucun lien
	Ami
	Voisin
	Ex-partenaire
	Collègue de travail
	Lien inconnu
	Autre (veuillez préciser)

(4) Cause de l'atteinte à la vie privée

À la lumière des premiers résultats de l'enquête, quelle serait selon vous la cause la plus probable de l'atteinte?

	Accident ou oubli
	Défaillance technique
	Vol ou acte répréhensible intentionnel
	Accès non autorisé aux fichiers
	Cause inconnue
	Autre (veuillez préciser)

(5) Étendue de l'atteinte à la vie privée

Combien de personnes sont concernées par l'atteinte?

	Très peu (moins de 10 personnes)
	Groupe cerné et limité (de 10 à 50 personnes)
	Groupe de plus de 50 personnes
	Nombre inconnu

(6) Préjudices prévisibles de l'atteinte

Déterminer les types de préjudice qui peuvent découler de l'atteinte à la vie privée en question. Certains préjudices se rapportent exclusivement aux personnes concernées, et d'autres peuvent être causés à la Société de la SP et à d'autres personnes si aucune notification n'est transmise :

	Indiquer le type de renseignements volés (surtout lorsqu'il s'agit du vol de numéros d'assurance sociale, de numéros de cartes de crédit, de numéros de permis de conduire, d'information sur des cartes de débit, etc.)
	Préjudice physique (p. ex. harcèlement criminel ou autre)
	Souffrance, humiliation, atteinte à la réputation (découlant de la divulgation de dossiers médicaux, disciplinaires ou sur la santé mentale, par exemple)
	Perte d'occasions d'affaires ou de possibilités d'emploi (causée habituellement par une atteinte à la réputation)
	Non-respect d'obligations contractuelles (certains contrats prévoient l'envoi d'une notification aux tierces parties en cas de perte de données ou d'atteinte à la vie privée)
	Autres atteintes à la vie privée attribuables à des défaillances techniques (l'envoi d'un avis au fabricant du matériel informatique peut s'avérer nécessaire si un rappel est justifié; cela pourrait également permettre d'éviter que d'autres utilisateurs soient victimes d'atteintes à la vie privée)
	Autre (veuillez préciser)

(7) Autres facteurs

La nature du lien entre la Société de la SP et les personnes concernées peut justifier la notification de ces personnes au sujet de l'atteinte à leur vie privée, quels que soient les autres facteurs impliqués, afin de préserver le lien de confiance qui unit ces personnes à la Société de la SP. Il est donc recommandé de tenir compte du groupe auquel ces personnes appartiennent.

	Participants aux programmes de la Société de la SP ou prestataires de services dispensés par la Société de la SP
	Donateurs
	Bénévoles

	Employés
	Autres (veuillez préciser)

D. Évaluation des risques

Établir le niveau de risque associé à chacun des facteurs mentionnés plus haut. L'**annexe D** peut servir de guide dans cette démarche :

Facteurs de risque	**Niveau de risque**		
	Faible	**Modéré**	**Élevé**
1) Limitation de l'atteinte			
2) Nature des renseignements personnels en cause			
3) Lien			
4) Cause de l'atteinte			
5) Étendue de l'atteinte			
6) Préjudices prévisibles			
7) Autres facteurs			
Niveau de risque global			

À l'aide de l'échelle de risque présentée à l'**annexe D**, évaluer la pertinence d'aviser les personnes concernées et élaborer des mesures de prévention d'autres atteintes. Le préjudice possible causé par l'atteinte s'avère généralement un facteur clé dans la prise de décision quant à la notification des personnes concernées.

En général, un niveau de risque modéré ou élevé justifie qu'on communique avec les personnes concernées, mais un faible risque peut aussi le justifier selon les circonstances entourant chaque cas.

E. Notification

1) Doit-on aviser les personnes concernées?

La décision d'aviser les personnes concernées doit être basée sur l'évaluation du niveau de risque global lié à l'atteinte à la vie privée. Si l'un ou l'autre des facteurs suivants s'applique, une notification doit être transmise.

Points à considérer	**Description**	**Facteur présent**
Dispositions de la loi		

Points à considérer	Description	Facteur présent
Risque de vol d'identité	L'atteinte est liée au vol de numéros d'assurance sociale, de numéros de cartes de crédit, d'information sur des cartes de débit, etc.	
Risque de préjudice physique	L'information divulguée peut entraîner un risque de préjudices physiques découlant par exemple de harcèlement criminel ou autre.	
Risque de souffrance, d'humiliation, d'atteinte à la réputation	Ce type de risque est souvent associé à la divulgation de dossiers médicaux, disciplinaires ou sur la santé mentale, par exemple.	
Perte d'occasions d'affaires ou de possibilités d'emploi	L'atteinte peut ternir la réputation professionnelle des personnes concernées.	
Explication requise	La Société de la SP peut décider d'aviser les personnes concernées lorsque ces personnes sont vulnérables ou si ces personnes souhaitent bien comprendre ce qui s'est passé, même si le niveau de risque a été jugé faible.	
Réputation de la Société de la SP	Lorsque la Société de la SP craint que l'atteinte puisse miner la confiance que ses parties prenantes ont en elle, elle peut décider d'aviser les personnes concernées de l'incident afin de calmer leurs inquiétudes et de bien les informer sur les risques liés à l'atteinte et sur les mesures d'atténuation des risques mises de l'avant, même si ces risques sont faibles.	

2) Quand faut-il notifier les personnes concernées, et quelle méthode de notification faut-il employer?

Quand : On doit notifier les personnes concernées le plus tôt possible après l'incident. Toutefois, si le dossier est entre les mains de la police, il se pourrait que les autorités policières vous demandent de retarder l'envoi de cet avis afin de ne pas nuire à une éventuelle enquête criminelle.

Comment : La méthode de notification privilégiée consiste à communiquer directement – par téléphone, par écrit ou en personne – avec les personnes concernées. La notification indirecte – affichage d'avis, diffusion de l'information sur le site Web ou par l'entremise d'annonces ou de communiqués de presse – devrait

généralement être réservée aux situations 1) où la notification directe pourrait aggraver le préjudice subi par les personnes concernées ou augmenter le coût de la démarche, et 2) où les coordonnées des personnes concernées ne sont pas disponibles. Dans certains cas, la méthode la plus efficace consiste à recourir à plusieurs méthodes de notification.

Facteurs militant en faveur d'une notification directe	**Cocher s'il y a lieu**
L'identité des personnes concernées est connue.	
Les coordonnées actuelles des personnes concernées sont disponibles.	
Les personnes concernées demandent des détails sur l'atteinte à leur vie privée afin de pouvoir se protéger contre tout préjudice qui pourrait en découler.	
Les personnes concernées peuvent avoir de la difficulté à comprendre une notification indirecte (en raison de leur état mental, de leur âge, de la langue utilisée, etc.).	
Facteurs militant en faveur d'une notification indirecte	
Un très grand nombre de personnes sont concernées par l'atteinte à la vie privée en question, de sorte qu'une notification directe pourrait s'avérer impossible.	
Une notification directe pourrait aggraver le préjudice subi par les personnes concernées.	

3) Contenu de la notification

Le contenu de la notification doit permettre aux personnes concernées d'atténuer ou de prévenir tout préjudice qui pourrait découler de l'atteinte à la vie privée. Il convient donc de fournir l'information suivante :

Éléments d'information à fournir absolument lors de la notification	**Fourni**
Date de l'atteinte.	
Description de l'atteinte.	
Description des renseignements personnels en cause.	
Mesures déjà prises par la Société de la SP pour limiter ou atténuer les préjudices.	
Mesures que les personnes concernées peuvent prendre pour se protéger elles-mêmes contre tout préjudice.	
Mesures que la Société de la SP compte prendre pour prévenir d'autres atteintes à la vie privée.	
Coordonnées de la Société de la SP – à l'intention des personnes qui voudraient obtenir de l'aide.	

4) Autres personnes ou organismes à aviser

Police ou organisme	Motif justifiant la notification	Motif applicable
Autorités policières	En cas de présomption de vol ou de crime.	
Assureurs	Lorsqu'une notification est requise en vertu d'un contrat d'assurance.	
Fournisseurs de technologies	Si l'atteinte à la vie privée est liée à une défaillance technique et à un rappel du fournisseur du matériel informatique ou si des correctifs techniques sont nécessaires.	
Autres (veuillez préciser)		

5) Confirmation de la notification

Principales personnes à aviser	Notification faite
Personne responsable de la protection de la vie privée de la division concernée	
Personne responsable de la protection de la vie privée du Bureau national	
Vice-président adjoint du marketing et des communications	
Vice-président des technologies de l'information	
Service des TI	
Président ou directeur général de la division concernée	
Président et chef de la direction de la Société de la SP	
Vice-président en chef des finances	
Police (s'il y a lieu)	
Personnes concernées	
Conseiller juridique	
Représentant du Commissariat à la protection de la vie privée du territoire concerné	
Autres (veuillez préciser)	

Annexe D

SOMMAIRE DES FACTEURS À PRENDRE EN CONSIDÉRATION DANS L'ÉVALUATION DES RISQUES

Le tableau suivant, qui se veut un guide dans l'évaluation des risques, résume les facteurs de risques liés aux atteintes à la vie privée et propose le niveau de risque possible présenté par chacun d'eux.

Guide d'évaluation des risques			
Facteur	**Niveaux de risque**		
	Faible	**Modéré**	**Élevé**
Nature des renseignements personnels en cause	✓ L'information était du domaine public et non liée à d'autres renseignements.	✓ L'information avait été recueillie par la Société de la SP et n'était pas de nature médicale ni financière.	✓ Il s'agissait de renseignements médicaux, relatifs au counseling ou sur la santé mentale, de données financières ou de numéros d'identification uniques attribués par le gouvernement.
Lien	✓ Les données ont été divulguées fortuitement par un professionnel de la santé à un autre qui a signalé l'atteinte à la vie privée; la destruction de ces données a été confirmée ou les données ont été récupérées.	✓ Les données ont été divulguées fortuitement à une personne inconnue qui a signalé l'atteinte à la vie privée; la destruction de ces données a été confirmée ou les données ont été récupérées.	✓ Les données ont été divulguées par une personne qui avait un lien avec les personnes concernées ou qui connaissait ces personnes, en particulier à des proches de personnes atteintes de SP, des voisins ou des collègues de travail motivés. ✓ Les données ont été volées par une personne inconnue.

Guide d'évaluation des risques			
Facteur	**Niveaux de risque**		
	Faible	**Modéré**	**Élevé**
Cause de l'atteinte à la vie privée	✓ Défaillance technique qui a été corrigée.	✓ Perte ou divulgation fortuite de données.	✓ Acte intentionnel. ✓ Cause inconnue. ✓ Défaillance technique qui n'a pas été corrigée.
Portée	✓ Très peu de personnes sont concernées.	✓ Le groupe de personnes concernées a été déterminé et est limité.	✓ Le groupe de personnes concernées est nombreux ou le nombre total de personnes concernées n'est pas déterminé (plus de 50 personnes).
Limitation de l'atteinte	✓ Les données étaient adéquatement cryptées. ✓ Les données ont été effacées à distance du dispositif de stockage portable où elles étaient sauvegardées, et tout indique que personne n'a accédé à ce dispositif après l'effacement des données. ✓ Les dossiers papier ou le dispositif de stockage portable ont été récupérés presque immédiatement	✓ Les données ont été effacées à distance du dispositif de stockage portable où elles étaient sauvegardées, dans les heures qui ont suivi l'incident, mais rien ne prouve que personne n'a accédé à ce dispositif après l'effacement des données. ✓ Les dossiers papier ou le dispositif de stockage portable ont été récupérés, mais suffisamment longtemps après l'incident pour	✓ Les données n'étaient pas cryptées. ✓ Les données, les fichiers ou le dispositif de stockage portable n'ont pas été récupérés. ✓ Les données risquent d'être divulguées à une échelle élargie en particulier par l'entremise des médias de masse ou par Internet.

Guide d'évaluation des risques			
Facteur	**Niveaux de risque**		
	Faible	**Modéré**	**Élevé**
	après l'incident, et il semble que tous les fichiers sont intacts ou qu'ils n'ont pas été lus ou les deux.	permettre l'accès aux données.	
Préjudices prévisibles découlant de l'atteinte à la vie privée	✓ Aucun préjudice prévisible.	✓ Perte d'occasions d'affaires ou de possibilités d'emploi. ✓ Souffrance, humiliation, atteinte à la réputation ou détérioration des relations. ✓ Préjudices sur le plan social ou relationnel. ✓ Perte de confiance envers la Société de la SP. ✓ Perte d'actifs subie par la Société de la SP. ✓ Perte de contrats ou d'occasions d'affaires subie par la Société de la SP. ✓ Risques financiers pour la Société de la SP, y compris les recours collectifs.	✓ Risques pour la sécurité des personnes concernées (p. ex. préjudices physiques). ✓ Risques de vol d'identité ou de fraude. ✓ Souffrance, humiliation et atteinte à la réputation peuvent être accrues selon les circonstances. ✓ Risques pour la santé ou la sécurité publiques.