Titre :	ATTEINTE À LA VIE PRIVÉE		**N° :** GEN.6.30.20
Section :	6. Gestion de l'information	**Date d'entrée en vigueur:**	**2010-12-15**
Émise par :	Directrice principale de l'Information et de la Protection des renseignements personnels	**Date de révision précédente :**	
Approuvée par (Signature)	Président-directeur général	**Date de la signature :**	2010-11-01
Établissement / programme : (facultatif)		☑ **Vitalité** **Zone(s)** ☐ 1 ☐ 4 ☐ 5 ☐ 6	

Il s'agit d'une politique conjointe du Groupe de travail des chefs de la protection de la vie privée. Elle ne peut être modifiée qu'avec le consentement de tous les membres du Groupe.

INTRODUCTION

Les régies régionales de la santé, FacilicorpNB et Ambulance NB, en tant que partenaires du système de la santé (ci-après appelés « partenaires »), s'engagent tous à recueillir, à utiliser, à divulguer et à éliminer les renseignements confidentiels, notamment les renseignements personnels (RP) et les renseignements personnels sur la santé (RPS), leur ayant été confiés, de façon à ce qu'ils soient exacts, confidentiels, protégés et privés.

OBJECTIF

La présente politique a pour but de présenter la démarche relative au signalement et à l'intervention en cas d'atteinte réelle ou présumée à la vie privée.

PORTÉE

La présente politique s'applique dans tous les cas où les employés des partenaires ou le personnel non-employé participent à des activités leur donnant accès à des renseignements personnels et des renseignements personnels sur la santé, et où une atteinte est réelle ou présumée.

PRESCRIPTIONS LÉGISLATIVES

Loi sur le droit à l'information et la protection de la vie privée (*LDIPVP*)
Loi sur l'accès et la protection en matière de renseignements personnels sur la santé (*LAPRPS*)

DÉFINITIONS

Une **« atteinte à la vie privée »** survient lorsqu'il y a évidence ou qu'il y a une possibilité élevée :

- d'accès,
- de collecte,
- d'utilisation,
- de divulgation,
- d'élimination

non autorisées des renseignements personnels ou des renseignements personnels sur la santé.

Le « **personnel non-employé** » comprend, sans toutefois s'y limiter, des agents, des membres du conseil d'administration, des étudiants, des bénévoles, des médecins, des consultants, des tiers fournisseurs de services, des professionnels ou des experts externes offrant un service sous contrat et des fournisseurs procédant à la démonstration, à l'installation ou à la réparation de l'équipement, des logiciels ou du matériel informatique.

Les **« renseignements personnels »** Renseignements consignés concernant une personne physique identifiable, notamment, sans toutefois, s'y limiter :

a) son nom;
b) l'adresse ou le numéro de téléphone ou de télécopieur de sa résidence, ou son adresse électronique à la maison;
c) son âge, son sexe, son orientation sexuelle, son état matrimonial ou familial;
d) son ascendance, sa race, sa couleur, sa nationalité ou son origine nationale ou ethnique;
e) sa religion ou sa confession ou sa croyance, son appartenance ou son activité religieuse;
f) les renseignements personnels sur la santé le concernant;
g) son groupe sanguin, ses empreintes digitales ou autres traits héréditaires;
h) son allégeance, son appartenance ou son activité politique;
i) son éducation ou sa profession ou ses antécédents scolaires ou professionnels;
j) sa source de revenus ou sa situation, ses activités ou ses antécédents financiers;
k) ses antécédents criminels, y compris ses infractions réglementaires;
l) ses opinions personnelles, sauf si elles ont trait à autrui;
m) les opinions d'autrui sur lui;
n) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre.

Les **« renseignements personnels sur la santé »** Renseignements identificatoires oraux ou sur un support quelconque se rapportant à une personne physique si l'information :

a) a trait à sa santé physique ou mentale, et ses antécédents familiaux ou en matière de santé, y compris son information génétique;
b) a trait à son inscription, y compris son numéro d'assurance-maladie;
c) a trait aux soins de santé qui lui sont fournis;
d) a trait aux paiements ou à l'admissibilité à des soins de santé ou à son admissibilité à ces soins ou à cette assurance;
e) a trait au don d'une partie de son corps ou d'une de ses substances corporelles ou qui sont dérivés de l'analyse ou de l'examen d'une telle partie ou substance, [sic] y compris des renseignements dérivés d'une analyse ou d'un examen d'ordre génétique la concernant;
f) identifie son mandataire spécial;
g) identifie son fournisseur de soins de santé.

ÉNONCÉ DE POLITIQUE

Les partenaires s'engagent à répondre à toute atteinte présumée ou réelle à la vie privée, au moment opportun, conformément aux modalités établies dans la présente politique.

Toute personne soupçonnant une atteinte doit immédiatement aviser son gestionnaire et le chef de la protection de la vie privée de son organisation.

MODALITÉS

Cinq étapes doivent être suivies au moment de répondre à une atteinte à la vie privée :

1. Limitation de l'atteinte à la vie privée et enquête préliminaire;
2. Notification interne/mise en œuvre de la politique en cas d'atteinte à la vie privée;
3. Évaluation des risques;
4. Notification des individus concernés et des autres;
5. Mesures correctives pour prévenir une atteinte future et le suivi des employés et du personnel non-employé

Nota : Les étapes 1 et 2 peuvent être effectuées simultanément.

Étape 1 : <u>Limitation de l'atteinte à la vie privée et enquête préliminaire</u>

Limitation de l'atteinte à la vie privée

La personne responsable de l'atteinte ou ayant découvert une atteinte réelle ou présumée, en consultation avec son superviseur et le chef de la protection de la vie privée, doit prendre sans tarder des mesures pour limiter l'atteinte à la vie privée. Ces mesures pourraient consister à :

- mettre fin à la pratique non autorisée;
- récupérer les dossiers et **<u>toutes</u>** les copies;
- éteindre le système qui fait l'objet de l'atteinte;
- révoquer ou changer les codes d'accès informatiques ou corriger les lacunes des systèmes de sécurité matériels ou électroniques;
- le superviseur devrait contacter le bureau des Ressources humaines (RH) pour déterminer si la situation justifie ou non une mesure disciplinaire.

Enquête préliminaire

Dès qu'il est avisé d'une atteinte réelle ou présumée, le chef de la protection de la vie privée, en consultation avec le gestionnaire, doit immédiatement entreprendre une enquête pour déterminer si une atteinte est survenue et la portée des renseignements personnels et des renseignements personnels de la santé mis en cause.

Il peut également être nécessaire de mettre en œuvre les mesures suivantes dans le cadre de l'enquête :

- Consulter des ressources externes, où et quand approprié.
- Identifier les individus à l'interne et à l'externe, qui doivent être avisés de l'atteinte et que l'enquête est en cours.
- Notifier la police s'il s'avère que l'atteinte concerne un vol ou une autre activité criminelle.
- Recueillir et conserver tous les éléments de preuve liés à l'atteinte. Ceci comprend ce qui suit :
    - Déterminer la portée de l'atteinte;
    - Conserver les renseignements personnels sur la santé en question;
    - Mener des entrevues et protéger les déclarations écrites ou les notes de personnes comportant des renseignements liés à l'atteinte;
    - Obtenir toutes les copies des documents (copies écrites, électroniques ou enregistrements);
    - Consigner toutes les procédures ou pratiques des parties concernées qui ne sont pas précisées par écrit.

Étape 2 : Notification interne/mise en œuvre de la Politique en cas d'atteinte à la vie privée

- Le personnel doit immédiatement aviser son gestionnaire de toute atteinte réelle ou présumée.et un rapport d'incident doit être rédigé. Dans le cas où le gestionnaire n'est pas disponible, le personnel peut contacter le chef de la protection de la vie privée directement;

- Le gestionnaire doit immédiatement informer le chef de la protection de la vie privée de son organisation. Selon la nature ou la gravité de l'atteinte présumée à la vie privée, le chef de la protection de la vie privée déterminera quel membre du personnel sera avisé et si les cadres supérieurs doivent être informé ou non de la situation;

- Quand il en est approprié, le chef de la protection de la vie privée du partenaire concerné informera le ministère de la Santé de l'atteinte à la vie privée dans les meilleurs délais;

- Le chef de la protection de la vie privée fournira une notification préliminaire au Commissaire à l'accès à l'information et à la protection de la vie privée, si appropriée ;

- Si une personne qui travaille dans une organisation devient consciente qu'une atteinte à la vie privée réelle ou présumée a lieu dans l'organisation d'un autre partenaire, elle avisera immédiatement son chef de la protection de la vie privée qui contactera le chef de la protection de la vie privée de l'organisation en cause.

Étape 3 : Évaluation des risques

Le chef de la protection de la vie privée, en consultation avec le gestionnaire chargé du secteur d'activité concerné, devra mener une enquête sur la cause de l'atteinte et l'ampleur des dommages résultant de l'atteinte pour la ou les personne(s) concernée(s) et toutes les autres personnes.

Étape 4 : Notification aux individus concernés et aux autres

Toutes les lois relatives au respect de la vie privée requièrent que les organisations mènent leurs affaires de façon transparente. Dans une situation d'atteinte à la vie privée, nous devons être tout aussi transparents en identifiant ce qui s'est passé. Cela signifie que, selon la situation et quand cela est recommandé, nous devons aviser différentes personnes qu'une atteinte a lieu, incluant les personnes dont il a été déterminé que la vie privée a été atteinte.

Étapes concernant la notification :

- Déterminer, en consultation avec le service des communications, si, quand et comment informer (par envoi direct par la poste ou par téléphone, par avis public, par l'intermédiaire des médias, d'Internet);
- Déterminer qui devrait communiquer avec les personnes concernées ou qui devrait leur envoyer la notification;
- Déterminer ce que la notification doit comprendre;
- Préparer la notification comme il convient.

Le chef de la protection de la vie privée avisera le Commissaire à l'accès à l'information et à la protection de la vie privée au besoin.

Étape 5 : <u>Mesures correctives pour prévenir des atteintes futures et suivis des employés et du personnel non-employé</u>

Une fois l'enquête terminée, le chef de la protection de la vie privée doit soumettre un rapport d'enquête aux cadres supérieurs. Le rapport doit inclure des *recommandations* de mesures correctives ayant pour but de prévenir des atteintes futures, y compris, au besoin :

- une vérification de la sécurité physique et technique;
- un examen des politiques et des procédures et les modifications recommandées qui témoignent des leçons tirées de l'enquête;
- un examen des pratiques de formation des employés et des recommandations;
- un examen des pratiques existantes des partenaires et mandataires de services qui aide à déterminer si des mesures correctives ou des améliorations sont requises;
- toutes les autres mesures considérées comme adéquates dans les circonstances par le chef de la protection de la vie privée.

Suivis des employés et du personnel non-employé

Employés

Le tableau A intitulé, « Atteintes à la vie privée et mesures disciplinaires possibles », identifie la nature progressive de la discipline requise lors des interactions avec les employés concernés par l'atteinte à la vie privée. Il est à **noter** que le **niveau de discipline** dans chaque situation sera déterminé au cas par cas, en prenant en considération toutes les circonstances et tous les facteurs pertinents.

En plus des mesures disciplinaires possibles à l'interne, un individu pourrait faire l'objet de sanctions juridiques pour avoir violé une loi provinciale. Cela constitue une infraction de catégorie F sous la *Loi sur la procédure applicable aux infractions provinciales*.

Personnel non-employé

Les gestionnaires du personnel non-employé doivent effectuer le suivi approprié et communiquer les résultats au chef de la protection de la vie privée.

Tableau A : Atteintes à la vie privée et mesures disciplinaires possibles

Les niveaux suivants d'atteinte à la vie privée peuvent être utilisés à titre de guide pour déterminer les mesures à prendre à la suite d'une atteinte réelle des renseignements personnels (RP) ou des renseignements personnels sur la santé (RPS).

Niveaux d'atteinte à la vie privée	Exemples d'atteintes à la vie privée	Mesures disciplinaires possibles
Niveau 1 – non intentionnelle Négligence lors du traitement des RP ou des RPS ou d'un maintien adéquat des niveaux de sécurité	▫ Communiquer des RP ou des RPS sans vérifier l'identité du demandeur. ▫ Laisser des RP ou des RPS sans surveillance ou dans un lieu public. ▫ Ne pas fermer un ordinateur qui contient des RP ou des RPS. ▫ Envoyer par inadvertance des RP ou des RPS par télécopieur à un mauvais numéro. ▫ Accéder de façon non autorisée à ses propres RP ou RPS ou à ceux d'un membre de la famille.	▫ Discussion au sujet des politiques et procédures pertinentes ▫ Formation sur la protection de la vie privée ou lettre d'attente ▫ Signer ou signer de nouveau une déclaration de confidentialité et de non-divulgation ▫ Réprimande verbale ou écrite consignée ▫ Dans des circonstances exceptionnelles, une mesure disciplinaire appropriée pouvant aller jusqu'à la suspension avec ou sans rémunération, voire un licenciement
Niveau 2 – intentionnelle, non malveillante Infraction des politiques ou de la loi relatives à l'utilisation et à la communication des RP et des RPS	▫ Accéder aux RP et aux RPS sans justification professionnelle ▫ Discuter des RP et des RPS avec une personne qui n'a pas un besoin légitime de les connaître ▫ Permettre à une autre personne d'utiliser son compte informatique ou son mot de passe ▫ Récurrence d'accès non autorisés à ses RP et ses RPS ou à ceux d'un membre de sa famille Infractions répétées de niveau 1	▫ Discussion au sujet des politiques et procédures pertinentes ▫ Formation sur la protection de la vie privée ou lettre d'attente ▫ Signer ou signer de nouveau une déclaration de confidentialité et de non-divulgation Une mesure disciplinaire appropriée pouvant aller jusqu'à la suspension avec ou sans rémunération, voire un licenciement
Niveau 3 – intentionnelle et malveillante Infraction en toute connaissance de cause des politiques ou de la loi relatives à l'utilisation et à la communication des RP ou des RPS pour un profit personnel ou pour faire du tort à d'autres personnes	□ Accéder à des RP ou à des RPS sans que cela figure dans les compétences professionnelles à des fins de profit personnel ou pour faire du tort à d'autres personnes (p. ex. : utiliser des renseignements dans le cadre d'un différend concernant la garde d'enfant ou d'une procédure de divorce). □ Utiliser le compte d'ordinateur d'un autre employé à des fins de profit personnel ou pour faire du tort à d'autres personnes. □ Modifier intentionnellement des données ou supprimer des RP ou des RPS quel que soit la forme. □ Infractions répétées de niveau 1 et 2.	▫ Mesure disciplinaire – suspension sans rémunération ou licenciement (l'employé est inadmissible à la réembauche) ▫ Révocation des privilèges du personnel médical et des privilèges d'accès.

RESPONSABILISATION

Chef de la protection de la vie privée est responsable de :

- Maintenir à jour les politiques, normes, procédures, lignes directrices et outils requis pour appuyer l'identification et la gestion efficaces des atteintes à la vie privée;
- Mettre en œuvre, interpréter la présente politique et en promouvoir la conformité;
- Documenter les résultats des enquêtes portant sur les atteintes à la vie privée;
- Établir des processus pour rapporter rapidement et régulièrement les atteintes à la vie privée et les résultats de toute enquête au président-directeur général;
- Surveiller la résolution des atteintes à la vie privée et les mesures correctives.

Employé et personnel non-employé sont responsables de :

- Signaler un risque d'atteinte à la sécurité ou à la vie privée au chef de la protection de la vie privée pour faciliter la prévention des atteintes;
- Signaler une atteinte réelle ou présumée à son gestionnaire et à son chef de la protection de la vie privée;
- Coopérer lors de l'enquête, au besoin; et
- Effectuer le suivi des risques identifiés d'atteinte à la sécurité ou à la vie privée pour améliorer la protection de la vie privée.

RÉFÉRENCES ET DOCUMENTS CONNEXES

- *Loi sur l'accès et la protection en matière des renseignements personnels sur la santé (LAPRPS)*
- *Loi sur le droit à l'information et la protection de la vie privée (LVIPVP)*
- Trousse d'évaluation des atteintes à la vie privée

DEMANDE DE RENSEIGNEMENTS

Pour de plus amples renseignements sur la présente politique, communiquez avec le chef de la protection de la vie privée de votre organisation :

AmbulanceNB
Nagesh Jammula (506) 872-6546

FacilicorpNB
Kelly Steeves (506) 663-2500

Réseau de santé Horizon
Nancy Lindsay (506) 375-2921

Réseau de santé Vitalité
Mireille Lanouette (506) 862-4205

Remplace :	**Zone 1 :** _____	**Zone 5 :** _____
	Zone 4 : _____	**Zone 6 :** _____