Manuel : Général du Réseau de santé Vitalité

Titre :	PARTAGE DE RENSEIGNEMENTS CONFIDENTIELS		**N° : GEN.6.30.30**
Section :	6. Gestion de l'information	**Date d'entrée en vigueur:**	**2015-03-18**
Émise par :	Directrice régionale de la Gestion intégrée des risques et chef régional de la Protection de la vie privée	**Date de révision précédente :**	2012-01-16
Approuvée par : (Signée par)	Président-directeur général Jean Castonguay	**Date de la signature :**	2015-03-18
Établissement / programme :		☑ **Vitalité Zone :** ❒ 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 (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 vise à prescrire les processus à mettre en œuvre pour le partage de renseignements personnels en tenant compte de la nature délicate desdits renseignements à partager.

PORTÉE

La présente politique s'applique dans tous les cas où les employés ou les membres du personnel non employé des partenaires participent à des activités leur donnant accès à des renseignements confidentiels, dont les renseignements personnels (RP) et les renseignements personnels sur la santé (RPS).

PRESCRIPTIONS LÉGISLATIVES

Les partenaires sont assujettis et doivent se conformer à la *Loi sur le droit à l'information et la protection de la vie privée (LDIPVP)* et à la *Loi sur l'accès et la protection de renseignements personnels sur la santé (LAPRPS)* et à leurs règlements.

DÉFINITIONS

Le « **personnel non employé** » comprend, sans toutefois s'y limiter, les membres du conseil d'administration, les agents, les étudiants, les bénévoles, les médecins, les consultants, les tiers fournisseurs de services, les 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 confidentiels** » comprennent les types de renseignements suivants, sans toutefois s'y limiter :

- Renseignements personnels (RP)
- Renseignements personnels sur la santé (RPS)
- Renseignements de nature délicate et des informations confidentielles (p. ex. renseignements administratifs notés dans des carnets ou des agendas personnels)
- Renseignements des ressources humaines ou de la paie
- Renseignements juridiques
- Renseignements financiers

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 la concernant;
g) son groupe sanguin, ses empreintes digitales ou autres traits héréditaires;
h) son allégeance, son appartenance ou son activité politique;
i) ses études ou son emploi 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 elle;
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 cette assurance;
e) a trait au don d'une partie de son corps ou d'une de ses substances corporelles ou à l'analyse ou l'examen d'une telle partie ou substance;
f) identifie son mandataire spécial; ou
g) identifie son fournisseur de soins de santé.

ÉNONCÉ DE POLITIQUE

Le partage de renseignements confidentiels ne doit avoir lieu que s'il est approprié et autorisé par la loi.

Les employés et les membres du personnel non employé sont responsables de leur manière de traiter les renseignements confidentiels, y compris les RP et les RPS; il leur incombe d'agir avec prudence lors du partage de renseignements personnels, y compris en ce qui a trait à la méthode d'envoi des renseignements afin de protéger la confidentialité et la vie privée.

Si une erreur est soupçonnée ou confirmée lors du partage de renseignements personnels, il faut la déclarer immédiatement au superviseur et au chef de la protection de la vie privée de son organisme, comme le précise la Politique sur les atteintes à la vie privée.

MODALITÉS

Pour déterminer le moyen le plus approprié de transmettre des renseignements confidentiels, y compris des RP et des RPS, la personne doit évaluer ses pratiques de communication en fonction de la présente politique et des autres pratiques exemplaires connues, le cas échéant.

Considérations générales pour le transfert de données/renseignements

1. Communication face à face

   La communication face à face de renseignements confidentiels doit avoir lieu dans un endroit sûr et privé comme un local entouré de murs séparatifs complets et muni d'une porte fermée. Si un tel local n'est pas disponible, faire preuve de discrétion et de bon jugement.

2. Personnel non employé

   Pour partager des renseignements confidentiels avec du personnel non-employé, il faut s'assurer que la personne ou l'entité a signé une Déclaration de confidentialité et de non-divulgation (se référer à la Politique sur la confidentialité).

   Dans le cas d'un contrat avec un tiers fournisseur de services, une entente de partage d'information peut être requise.

L'entente de partage d'information doit être préparée en consultation avec le Bureau de la vie privée.

3. Transport de renseignements confidentiels en format papier

Limiter le transport de renseignements personnels en format papier ***au sein de son établissement*** et prendre les précautions suivantes :

- Insérer les renseignements dans une chemise à bouts fermés, une enveloppe de courrier interne ou placer ces renseignements sur une planchette à pincette avec un couvercle ou dans une boîte avec un couvercle de manière à ce qu'ils ne soient pas facilement visibles.
- Éviter d'inscrire des RP ou des RPS sur l'enveloppe, sauf ceux qui sont nécessaires à la livraison des renseignements.

Les dossiers de patients dans les établissements de santé ne doivent jamais quitter l'établissement à moins d'une ordonnance de la cour ou d'une permission exceptionnelle du service des archives cliniques. Les dossiers de patients utilisés par les services communautaires tels que la Santé publique, le Programme extra-mural et les centres de santé mentale peuvent être apportés dans la communauté selon leurs politiques respectives.

Limiter le transport de renseignements confidentiels en format papier ***à l'extérieur de votre établissement***. De plus, il est recommandé de prendre les précautions additionnelles suivantes :

- Veiller à ce que les documents confidentiels ne soient pas égarés en ayant un processus de localisation enregistrant la sortie et le retour des informations dans son lieu d'entreposage désigné.
- Transporter le minimum de renseignements confidentiels requis.
- Transporter les RPS de manière sûre, comme dans un porte-documents verrouillé, placé dans le coffre arrière d'un véhicule verrouillé.
- Éviter de laisser des renseignements confidentiels sans surveillance dans un véhicule, surtout pendant la nuit.

Pour Ambulance Nouveau-Brunswick, les dispositions ci-dessus sont sans objet en raison de la nature du travail. Pour leur transfert, les renseignements confidentiels peuvent ou non être dissimulés dans une chemise ou une enveloppe.

4. Courrier

4.1 Courrier interne

4.1.1 Envoyé à l'intérieur de l'établissement :

- Le courrier de nature confidentielle destiné à un autre secteur du même établissement doit être placé dans une enveloppe interservices ou dans une enveloppe scellée à la source. Le nom et le service du destinataire doivent être indiqués clairement sur l'enveloppe. On ne peut inscrire des RPS sur l'enveloppe ou y apposer une étiquette de patient.

- Pour ce qui est des documents confidentiels **déposés directement dans la case d'un médecin** par un membre du personnel du Réseau, ils doivent être pliés et on doit indiquer clairement le prénom et le nom de famille du médecin à qui ils sont destinés.

4.1.2 Envoyé vers un autre établissement du Réseau :

- Le courrier contenant de l'information confidentielle, des RP ou des RPS destiné à un autre établissement du Réseau et livré par FacilicorpNB doit être placé dans une enveloppe scellée à la source, adressée au destinataire avec son nom complet, le nom de son service et celui de l'établissement. Les coordonnées de l'expéditeur doivent également être inscrites sur l'enveloppe. La mention « Confidentiel » doit être apposée sur l'enveloppe.

4.2 Courrier régulier

Pour transmettre des RPS, des RP ou des renseignements confidentiels par l'entremise d'une salle de courrier (courrier interne, par la poste ou par une compagnie), les étapes suivantes doivent être suivies :

- L'information doit être insérée dans une enveloppe à usage unique, scellée à la source (avant l'envoi à la salle de courrier);
- Le nom complet (prénom et nom de famille) du destinataire, le nom de son service et son adresse complète doivent être inscrits sur l'enveloppe;
- Les coordonnées de l'expéditeur (nom et adresse de retour) doivent également être inscrites sur l'enveloppe;
- La mention « Confidentiel » doit être apposée sur l'enveloppe.

Si le document ou paquet est envoyé par courrier recommandé ou par une compagnie de livraison, il doit pouvoir être repéré (numéro de repérage).

5. Téléphone

En général, les lignes terrestres sont considérées comme un moyen sûr de transmettre des renseignements confidentiels, à la condition que le téléphone se trouve dans un endroit sûr et privé.

Les téléphones sans fil, les téléphones cellulaires, Blackberry ou tout autre type de téléphones intelligents ou téléphones satellites ne sont pas considérés comme complètement sûrs; par conséquent, à moins de ne pas avoir d'autre moyen de communication à sa portée, on doit limiter au minimum les renseignements identifiables donnés par téléphone.

Lorsque vous essayez de joindre un patient et que vous devez laisser un message vocal, laissez sur la boîte vocale juste assez de renseignements utiles pour le patient, comme :

- Votre nom
- Le lieu d'où vous téléphonez (Ne pas précisez le nom du programme ou le titre de fournisseur de services; vous pouvez donner le nom du Réseau.)

- Renseignements de base au sujet de l'appel (rappel au sujet d'un rendez-vous ou changement de l'heure d'un rendez-vous)
- Le message ne devrait pas contenir des renseignements précis au sujet d'un rendez-vous, y compris la nature et le lieu du rendez-vous, sauf si le patient a donné son consentement à un message plus détaillé ou s'il en a fait la demande.
- Un numéro de rappel

Voici un exemple :

Ici (Votre nom), du Réseau de santé Vitalité. C'est un message pour (nom du patient) au sujet du rendez-vous qui aura lieu le _____ à ____h. Veuillez me rappeler au (numéro) pour confirmer que vous assisterez à votre rendez-vous ou pour fixer une autre date si vous ne pouvez pas assister à votre rendez-vous. Merci.

Lorsqu'un service de rendez-vous doit communiquer avec le patient par téléphone à court préavis et qu'il doit laisser un message vocal, il lui est permis de nommer le service en question dans le message.

Lorsqu'un appelant externe demande des informations sur un client, les RPS sur le client peuvent uniquement être discutés lorsque l'identité du demandeur peut être confirmée par le personnel soignant en exigeant 2 identifiants et que ce dernier a obtenu le consentement préalable de la part du client qui autorise le partage de ses informations avec le demandeur.

6. Télécopieur

Avant de transmettre des renseignements confidentiels par télécopieur, il faut à tout le moins respecter le processus général suivant :

- Les télécopies doivent comporter une feuille d'envoi comprenant un avis de confidentialité dans le cas de renseignements personnels reçus par erreur. Par exemple, un avis de non-responsabilité tel le suivant peut être utilisé :

Avis de confidentialité

Cette télécopie et les pièces jointes peuvent contenir des renseignements confidentiels et privilégiés destinés seulement à l'usage du destinataire. La divulgation et la reproduction des informations contenues dans ces documents sont interdites. Si vous recevez cette télécopie par erreur, veuillez aviser l'expéditeur mentionné ci-dessous. Merci.

506 - _____ Nom : _____

- La feuille d'envoi doit comporter le nom du destinataire, la date, le numéro de télécopieur de la destination, le nombre total de pages et toute directive spéciale ainsi que le numéro de téléphone et le nom de l'expéditeur en cas de besoin ; aucun RP ou RPS doit être inclus sur la feuille d'envoi;
- L'expéditeur doit utiliser les numéros préprogrammés pour réduire les erreurs;
- L'expéditeur doit revérifier le numéro de télécopieur du destinataire;

- Dans des circonstances de nature extrêmement délicate telles que celles relatives à la santé mentale ou sexuelle, l'expéditeur doit prévenir le destinataire de l'envoi du document par télécopieur et lui demander d'en confirmer la réception. Lorsque possible, utiliser l'option d'impression confidentiel lorsque la télécopie contient des renseignements sensibles;
- De plus, dès réception de la confirmation de la transmission, l'expéditeur doit aussi vérifier que le numéro de télécopieur indiqué est le numéro de télécopieur voulu;
- Le télécopieur doit être localisé dans un endroit sûr.

La **télécopie par courriel** est un autre moyen de transmettre des renseignements confidentiels. Ce moyen limite l'accès aux renseignements personnels à l'extrémité de réception et il est considéré comme une option plus sûre que la transmission entre télécopieurs. Toutefois, pour assurer la sécurité du transfert, l'expéditeur devrait revérifier l'adresse courriel avant de procéder à l'envoi et demander un avis de réception de l'expéditeur.
Note : Lorsqu'on utilise la télécopie par courriel, il se peut que le message soit envoyé dans le fichier « pourriels » du destinataire. Faire preuve de précaution.

Transmission ou réception de transmission non intentionnelle

Si une télécopie confidentielle a été envoyée au mauvais destinataire, l'expéditeur doit :

- Communiquer avec le destinataire pour le prévenir de l'erreur;
- Communiquer avec le chef de la protection de la vie privée pour déclarer l'incident;
- Demander au destinataire non intentionnel de détruire le document de manière sûre et confirmer verbalement la destruction.

Si l'on reçoit une télécopie confidentielle par erreur, il faut :

- Communiquer avec l'expéditeur pour le prévenir de l'erreur;
- Communiquer avec le chef de la protection de la vie privée pour déclarer l'incident;
- Détruire le document selon les directives de l'expéditeur et confirmer sa destruction.

7. <u>Impression de renseignements confidentiels</u>

- L'imprimante doit se trouver dans un endroit sûr;
- Récupérer immédiatement les documents contenant des renseignements confidentiels que l'on transmet à une imprimante;
- Faire preuve de vigilance en envoyant des documents contenant des renseignements confidentiels à une imprimante située ailleurs. Utiliser une option d'impression confidentielle, lorsque disponible sur les imprimantes, vérifier et confirmer le numéro ou le code, ou encore s'assurer qu'une personne est disponible pour récupérer l'information sont des mesures qui peuvent assurer la transmission sûre de cette information. Pour utiliser l'option d'impression

confidentielle sur la plupart des imprimantes, appuyer sur le bouton « imprimer », suivi par le bouton « propriétés ».

8. Transfert électronique de renseignements confidentiels

L'information confidentielle de l'organisation ne devrait jamais être transférée à un appareil qui ne vous a pas été fourni par le Réseau.

8.1 Courrier électronique

En général, le courrier électronique ne peut pas être considéré comme un moyen entièrement sûr de transmettre des renseignements confidentiels. Toutefois, comparativement à d'autres moyens de partage de renseignements, **l'envoi de courrier électronique au sein d'un même réseau n'est pas considéré comme étant à risque élevé sur le plan technique.**

Voici l'adresse des « réseaux fiables » pour communiquer les uns avec les autres :

- prénom.nom de famille@horizonnb.ca
- prénom.nom de famille@vitalitenb.ca
- nom@facilicorpNB.ca
- nom@nbed.nb.ca
- nom@gnb.ca

Dans le cas d'AmbulanceNB, seuls les courriels internes sont permis (p. ex. : à et de nom@anb.ca et nom@smunbems.ca seulement).

Pour assurer l'intégralité du dossier du patient, qui est le document légal, les échanges par courrier électronique doivent se limiter au strict minimum et l'information clinique doit être consignée au dossier du patient.

Voici les pratiques exemplaires en matière d'envoi de courriels :

- Avant d'envoyer un message, vérifier si le destinataire (ou les destinataires) est bel et bien le destinataire voulu;
- La ligne de mention objet ne doit contenir aucun renseignement personnels ou renseignement personnels sur la santé ;
- Il faut faire preuve de prudence lorsque l'on adresse un message à des destinataires faisant partie d'une liste de distribution en s'assurant qu'ils sont tous autorisés à recevoir cette information et qu'elle leur est effectivement destinée ;
- Indiquer que l'information est de caractère « confidentiel » en inscrivant cette mention au tout début du corps du courriel;
- Si l'on transmet un message à quelqu'un par accident, essayer de « rappeler » le courriel. L'efficacité de la fonction de rappel des courriels est limitée, et il ne faut donc pas s'y fier. Il faut envoyer au destinataire non intentionnel un courriel lui expliquant qu'il a reçu un message par erreur et qu'il doit l'effacer en permanence immédiatement;

- Si de multiples destinataires ont reçu le message et qu'un destinataire a été inclus par erreur, demandez à tous les destinataires d'éliminer le destinataire non intentionnel avant d'utiliser la fonction « Répondre à tous »;
- Pour partager des RPS par courriel au sein d'un même réseau sécurisé, le chiffrement n'est pas obligatoire, mais il faut faire preuve de vigilance.

Envoi de courriels à l'extérieur de l'organisme

L'envoi de courriels contenant des RPS à l'extérieur des réseaux fiables **n'est pas** sûr, et il faut donc prendre les mesures suivantes :

- Inclure un avis de confidentialité bilingue dans toutes les transmissions électroniques faites à l'extérieur de son réseau;
- Pour partager des RPS par courriel à l'extérieur des réseaux fiables (énumérés ci-dessus), utiliser le cryptage, à moins que l'une des deux conditions suivantes soit remplie :

i) Le patient a consenti à la communication avec l'usager par courrier électronique. La relation entre le dispensateur de soins de santé et le patient devrait être déjà établie.
ii) Le courriel est nécessaire pour un échange unique entre des dispensateurs de soins de santé pour des raisons de santé urgentes. Dans un tel cas, l'expéditeur doit assurer un suivi en utilisant un autre moyen de communication, comme le téléphone, afin de s'assurer que l'information est parvenue au destinataire prévu et est traitée comme il se doit.

- Des renseignements personnels sur la santé non cryptés ne doivent pas être envoyés par courrier électronique sur Internet à l'adresse électronique à domicile d'un employé afin de permettre à cet employé de faire le travail à son domicile.

Envoi de courriels aux patients et réception de courriels des patients

Les dispensateurs de soins autorisés peuvent communiquer avec les patients par courrier électronique pour assurer les soins à ces patients, lorsque les conditions suivantes sont remplies :

1. Le directeur de programme ou le gestionnaire doit définir le type d'information qui peut être communiqué par courriel et obtenir l'autorisation auprès du chef de la protection de la vie privée de son organisation.

2. Les dispensateurs de soins désirant utiliser le courrier électronique pour communiquer avec des patients doivent établir par écrit avec le patient l'objet des échanges (p. ex., établissement d'un rendez-vous, renouvellement d'une ordonnance) et le niveau de sensibilité des sujets pouvant être envoyés par courriel, tout en respectant la politique établie par le programme.

3. Les dispensateurs de soins doivent obtenir un consentement explicite (écrit) de chaque patient pour communiquer avec lui par courrier électronique. Le consentement doit être obtenu en personne au moment du rendez-vous du

patient. Si la relation entre le dispensateur de soins et le patient est de longue date et que les rendez-vous du patient sont peu fréquents, le consentement peut être obtenu par courrier. Il n'est pas permis d'échanger aucune information par l'entremise de courriels avant d'avoir obtenu, en personne et au préalable, le consentement écrit.

4. Une copie signée du consentement doit être versée au dossier de santé du patient.

5. Une fois qu'ils ont obtenu le consentement du patient relativement aux communications par courrier électronique, les dispensateurs de soins doivent respecter les directives suivantes :
   - Consigner le contenu clinique pertinent de toute communication (message électronique, téléphone, etc.) dans les notes de progrès au dossier du patient.
   - Demander aux patients d'inscrire l'objet de l'échange dans la ligne de mention objet du message électronique, p. ex., prescription, rendez-vous, consultation médicale ou question par rapport à la facturation.

8.2 Message texte

Ce moyen de communication ne devrait pas être utilisé pour échanger des informations confidentielles, à moins que le message texte ne soit la seule façon de communiquer avec le patient, et le message ne devrait contenir que le minimum de renseignements requis. Avant d'avoir recours à ce type de communication, un consentement éclairé et écrit doit être obtenu du patient.

8.3 Transfert électronique de données

Lorsque l'on transfère des données par voie électronique, il faut avoir recours à des dispositifs de protection adéquats. Un contact devrait être établi avec le Service informatique pour déterminer le moyen à utiliser pour le transfert.

Les meilleures pratiques comportent les éléments suivants :
- Protection par mot de passe – l'expéditeur devrait transmettre le mot de passe au destinataire par un autre moyen;
- Utilisation d'un disque partagé à accès restreint;
- Observation d'un protocole de transfert de fichiers convenable, tel *Secure File Transfer Protocol* (SFTP), tunnel du réseau privé virtuel (tunnel du RPV), etc.;
- Utilisation de la technologie de cryptage des données.

8.4 Modem à numérotation automatique ou réseau (pas à haute vitesse)

Un modem à numérotation automatique passe par les lignes téléphoniques pour transférer des données d'un ordinateur à l'autre. Il s'agit d'un moyen acceptable pour transférer des données confidentielles entre des personnes, pourvu que le modem à numérotation automatique soit directement relié au serveur ou à l'hôte

désigné. Un modem à numérotation automatique relié à un fournisseur d'accès Internet n'est PAS un moyen acceptable pour transférer de l'information, sauf si l'on utilise un logiciel de chiffrement.

RESPONSABILITÉS

La responsabilité de la gestion des RPS relève du président-directeur général de chaque partenaire. Le chef de la protection de la vie privée de chaque partenaire a été chargé d'agir au nom de son président-directeur général.

Chaque **partenaire** a la responsabilité :

- De voir à la disponibilité des ressources pour assurer l'observation des politiques et procédures sur la protection de la vie privée.

Le **chef de la protection de la vie privée** a la responsabilité :

- D'assurer le maintien de politiques et d'outils pour préserver la confidentialité et appuyer des moyens efficaces pour le partage de l'information;
- D'aider à déterminer les risques en matière de vie privée et de sécurité ainsi que les stratégies d'atténuation.

Les **gestionnaires** ont la responsabilité :

- De déceler les risques en matière de vie privée et de sécurité dans leur secteur d'activité et d'adopter les stratégies d'atténuation qui s'imposent.
- Assurer le respect des politiques et procédures liées à la protection de RP et de RPS.

Les **employés et les membres du personnel non employé des partenaires** ont la responsabilité :

- De se conformer à la présente politique dans les tâches quotidiennes de collecte et de traitement des RP et des RPS dans la mesure où le partenaire juge que cela s'applique dans leur cas. Conformément à ses politiques et procédures en matière de discipline et d'approvisionnement, un partenaire peut imposer des sanctions aux employés ou aux membres du personnel non employé qui contreviennent à la présente politique alors qu'ils agissent en son nom.

RÉFÉRENCES ET DOCUMENTS CONNEXES

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

DEMANDE DE RENSEIGNEMENTS

Pour de plus amples renseignements sur la présente politique, communiquez avec la personne responsable de de la protection de la vie privée pour votre organisation.