
NBPPIA-2008-01

**ENQUÊTE SUR LA PERTE DES RENSEIGNEMENTS PERSONNELS PAR LE
MINISTÈRE DE LA SANTÉ – CARTOUCHES DES DONNÉES DE
FACTURATION DE L'ASSURANCE-MALADIE**

avril 2008

1.0 Introduction

Les résidents du Nouveau-Brunswick chérissent leur vie privée. Comme la plupart des Canadiens, ils considèrent que les renseignements personnels sur la santé se trouvent parmi les renseignements les plus délicats qu'ils possèdent. Ils ont des attentes très élevées à l'égard de la protection de ces renseignements et veulent que ceux-ci soient protégés jalousement.

La profession médicale et tous les arts de guérir reposent sur une relation de confiance qui commence par un respect sain de la protection des renseignements personnels des patients. La loi respecte également la norme de prudence élevée qui doit être exercée dans le traitement des renseignements personnels, comme les renseignements sur la santé, puisqu'ils peuvent révéler des secrets intimes au sujet des antécédents ou de l'état d'une personne et qu'ils se rapprochent très près des renseignements d'ordre biographique la concernant. Pendant que les pressions s'intensifient pour réaliser des gains d'efficacité dans le secteur des soins de santé et que les nouvelles technologies favoriseront l'élaboration de dossiers de santé électroniques, les résidents du Nouveau-Brunswick seront exposés à un grand nombre de nouveaux risques et de nouvelles menaces à leur vie privée et à la protection de leurs renseignements personnels sur la santé. Voilà pourquoi la province envisage d'adopter un nouveau cadre législatif pour garantir que la confidentialité des patients sera maintenue et renforcée, espérons-le.

Il est donc regrettable que nous ayons été obligés de faire enquête dans ce contexte même sur une atteinte à la vie privée au ministère de la Santé qu'il aurait été facile d'éviter. La plupart des atteintes à la vie privée déclarées au Canada surviennent à cause d'une erreur involontaire. Dans ce cas, le service d'expédition a perdu des cartouches des données de facturation de l'Assurance-maladie en transit. L'enquête n'a révélé aucune preuve de malveillance ou de faute, et la perte, même si elle n'a toujours pas été expliquée, semble être survenue par inadvertance. La vraie histoire, cependant, est la raison pour laquelle les renseignements ont été transférés de cette manière pour commencer et, ce qui est plus troublant encore, pourquoi est-ce que cela a pris tellement de temps avant que la perte soit découverte et fasse l'objet de mesures. Notre enquête a révélé que, en dépit de la promesse tant annoncée par le ministère de la Santé de protéger la vie privée des patients, il semble y avoir un manque d'engagement à l'égard de la protection de la vie privée au bureau central du Ministère qui a mené à cette atteinte.

L'élaboration de politiques dans ce domaine faisait crûment défaut. Il n'y avait pas de centre de responsabilité pour aider le sous-ministre à s'acquitter des fonctions en matière de responsabilité en vertu de la *Loi sur la protection des renseignements personnels (LPRP)*. Le personnel de première ligne et les cadres intermédiaires n'avaient aucune idée du fait que même un manieur de courrier, qui n'ouvre jamais de colis et qui n'a aucun accès aux dossiers médicaux personnels, a des obligations en vertu de la LPRP et des responsabilités primordiales afin de maintenir les dispositifs de protection pour

protéger de façon adéquate la confidentialité entre le médecin et le patient, ou l'infirmière et le patient.

Dans ce contexte, lorsque le chat est finalement sorti du sac, l'hyperbole et l'hystérie ont témoigné de façon aussi éloquente de la confusion et du manque de connaissances au sujet de la façon de procéder, que le manque fondamental de préparation et de politiques et de dispositifs de protection ne l'a fait. Chaque jour, on a réclamé la démission du ministre, ce qui a été suivi immanquablement par des mises à jour quotidiennes par le ministre au sujet de la situation à l'Assemblée législative. Tous se sont mis à pointer du doigt. Était-ce l'Assurance-maladie du Nouveau-Brunswick qui était en faute ou BC Health? Existait-il un problème dans l'ensemble du système, ou s'agissait-il d'une erreur dont seulement quelques-uns devraient rendre compte?

Cette enquête a révélé que, en fait, cela ne donne rien d'attribuer le blâme dans ce contexte au service de messagerie ou aux employés individuels. Dans tous les cas, il est ressorti que ces personnes accomplissaient leurs fonctions conformément à la politique existante et à une pratique de longue date. Ce qui manquait, c'était des politiques et des dispositifs de protection adéquats afin d'établir la culture de protection de la vie privée que les dix principes de la LPRP sont censés insuffler dans notre administration publique.

Les quelques pages suivantes présenteront plus en détail le contexte de la plainte, les constatations de notre enquête et quelques recommandations initiales que le Ministère devrait mettre en œuvre en temps voulu pour hausser la barre et pour insister avec plus de rigueur pour que tous ses employés s'acquittent de leurs obligations en vertu de la LPRP et en prévision d'obligations plus rigoureuses qui suivront en vertu d'une nouvelle loi sur la protection des renseignements personnels sur la santé.

2.0 Contexte

L'assurance-maladie est un système de facturation. Lorsque les résidents du Nouveau-Brunswick, à l'aide d'une carte d'assurance-maladie valide, ont accès aux services, les médecins et les autres professionnels de la santé communiquent l'information sur la facturation au ministère de la Santé afin d'être payés pour le service offert. Lorsqu'un résident du Nouveau-Brunswick reçoit des services dans les autres provinces, celles-ci se tournent vers la province du Nouveau-Brunswick pour se faire rembourser le coût de ces services. Le Nouveau-Brunswick a signé des ententes (de facturation réciproque intergouvernementale) avec l'ensemble des autres provinces et territoires (autres que le Québec) pour recouvrer ces coûts. Les provinces et les territoires échangent des renseignements entre eux au sujet des services qui ont été offerts aux résidents de l'extérieur de la province, à des intervalles définis. Cet échange peut se produire à une fréquence plus ou moins grande, selon le volume de renseignements.

Les renseignements qui sont échangés entre les provinces comprennent le nom, le numéro d'assurance-maladie, la date de naissance et le sexe du patient avec les codes de facturation. Chaque province a conclu une entente avec le gouvernement du

Nouveau-Brunswick au sujet de la transmission de renseignements. Lors de cette enquête, l'Alberta, le Manitoba, Terre-Neuve-et-Labrador, l'Ontario et l'Île-du-Prince-Édouard transmettaient ces renseignements par la voie d'un CD chiffré. Le Yukon, le Nunavut et les Territoires du Nord-Ouest envoyaient les renseignements sur support papier. Jusqu'en décembre 2007, la Colombie-Britannique les envoyait par cartouche. Le Nouveau-Brunswick et la Nouvelle-Écosse échangeaient les renseignements à l'aide de FTP (le protocole de transfert de fichier sur l'Internet).

Avant décembre 2007, le processus pour transmettre les renseignements à la Colombie-Britannique était le suivant. La Colombie-Britannique créait la cartouche qui contient la liste des services que les résidents du Nouveau-Brunswick ont reçus lorsqu'ils étaient en Colombie-Britannique. Le ruban non chiffré était envoyé au centre des données du Nouveau-Brunswick (qui est la responsabilité du ministère de l'Approvisionnement et des Services) où se trouve la base de données de l'Assurance-maladie. Le centre de données, qui est exploité par un entrepreneur indépendant, avisait la Direction de l'Assurance-maladie de l'arrivée du ruban. Les cartouches étaient envoyées au bibliothécaire responsable des rubans qui les conservait afin de les traiter. Le ruban était traité durant le passage de la facturation mensuel. Après son traitement, le ruban était retourné à la bibliothèque de rubans où il était emballé par le bibliothécaire en vue de le retourner en Colombie-Britannique avec les autres cartouches qui pouvaient contenir les mêmes renseignements au sujet des résidents de la Colombie-Britannique qui avaient reçu des services au Nouveau-Brunswick pour lesquels le Nouveau-Brunswick voulait se faire rembourser.

Le 3 octobre 2007, un entrepreneur du ministère de l'Approvisionnement et des Services du Nouveau-Brunswick a envoyé quatre cartouches contenant les renseignements sur les patients et sur la facturation à Health Insurance BC (HIBC) à l'aide d'un service de messagerie. Le 25 octobre 2007, HIBC a informé le ministère de la Santé que le colis n'était pas arrivé et lui a demandé le nom du service de messagerie. HIBC a communiqué avec le service de messagerie pour déterminer où se trouvait le colis. Le service de messagerie a informé HIBC que le colis manquait. Les cartouches contenaient des renseignements sur la facturation de l'Assurance-maladie concernant 485 résidents du Nouveau-Brunswick et 149 résidents de la Colombie-Britannique. Le 26 octobre, le personnel du ministère de la Santé a demandé à l'entrepreneur de créer une autre cartouche. La cartouche recréée a été envoyée à HIBC le 31 octobre 2007 et est arrivée sans danger.

C'est seulement le 29 novembre que la haute direction du Ministère a été informée par courriel sur un sujet connexe de la perte des cartouches contenant les renseignements personnels. Le cadre supérieur en question était alors à l'extérieur de la province et a lancé une enquête interne sur les cartouches manquantes.

Le 10 décembre 2007, le Bureau de l'ombudsman a appris du Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique que les cartouches avaient été égarées. Le bureau a donc communiqué avec le ministère de la Santé et a entrepris d'enquêter sur l'atteinte à la vie privée.

En plus d'une enquête sur les cartouches perdues, le ministre de la Santé a demandé à mon bureau de mener un examen de toutes les politiques et pratiques concernant la collecte, l'utilisation et la divulgation de renseignements personnels par le ministère de la Santé afin de déterminer si elles étaient adéquates. Je félicite le ministre d'avoir déterminé qu'un examen s'imposait. Après avoir examiné sa demande, j'ai informé le ministre que, compte tenu du volume élevé de travail qui demanderait un apport de ressources considérables et de la nécessité que le bureau maintienne son indépendance, il serait plus à propos que le Ministère ait recours à des ressources externes pour mener l'examen. J'ai offert l'aide de mon bureau pour 1) aider ses fonctionnaires à rédiger la demande de propositions (DP) portant sur de telles ressources; 2) recevoir et commenter les rapports d'étape; 3) examiner et commenter les recommandations reçues; et 4) offrir un encadrement durant la mise en œuvre.

Je réserverai mes commentaires au sujet de l'examen plus étendu au moment approprié et je limiterai ce rapport aux questions liées à la protection de la vie privée découlant de cette atteinte précise.

3.0 Analyse

3.1 La Loi

Le paragraphe 2(1) de la *Loi sur la protection des renseignements personnels* assujettit chaque organisme public au Code de pratique statutaire prévu à l'Annexe A de la *Loi* et est interprété conformément à l'Annexe B. Le ministère de la Santé est l'un des organismes auxquels s'applique la loi. Le Code de pratique statutaire est fondé sur les 10 principes de protection de la vie privée qu'a établis l'Association canadienne de normalisation (ACNOR) : 1) responsabilité; 2) détermination des fins de collecte; 3) consentement; 4) limitation de la collecte; 5) limitation de l'utilisation, de la divulgation et de la conservation; 6) exactitude; 7) dispositifs de protection; 8) transparence; 9) accès individuel; et 10) possibilité de porter plainte contre le non-respect des principes. Les deux principes qui concernent cette situation en particulier sont le principe 1 : responsabilité et le principe 7 : dispositifs de protection.

Le principe 1 à l'Annexe A prévoit qu'« [U]n organisme public est responsable des renseignements personnels dont il a la gestion. Le directeur exécutif d'un organisme public et ses représentants doivent s'assurer du respect par l'organisme public des principes suivants ». Il n'y avait aucune politique de protection de la vie privée au ministère de la Santé qui désignait une personne responsable du respect des principes de protection de la vie privée; donc ce rôle incombe au sous-ministre à titre de directeur exécutif.

Le principe 7 à l'Annexe A prévoit que « [L]es renseignements personnels doivent être protégés par des dispositifs de protection correspondant à leur degré de sensibilité ». L'Annexe B entre dans les détails en indiquant que « [L]es dispositifs de protection qui doivent être adoptés comprennent des mesures de formation et des mesures administratives, techniques, physiques et autres, comme il convient dans les circonstances, et comprennent les dispositifs de protection qui doivent être adoptés quand un organisme public divulgue des renseignements personnels à un tiers ou prend des mesures pour qu'un tiers recueille des renseignements personnels en son nom ».

3.2 Gravité de l'atteinte

Les renseignements en question ont été envoyés par cartouche. Les renseignements sur la cartouche comprenaient le nom, la date de naissance et le sexe du patient, la date du service, le code du service (code numérique), le code du diagnostic (code numérique), le numéro et le code de spécialité du praticien. Afin de comprendre quel service a été offert par le praticien, il faudrait avoir accès à la liste des codes avec leurs explications.

Selon la direction des TI au ministère de la Santé, afin de lire les cartouches, il faut avoir un lecteur, un contrôleur de lecteur, un ordinateur central ou intermédiaire et un logiciel spéciaux. Comme l'a indiqué le ministère de la Santé, cette technologie était seulement utilisée couramment dans les centres des données et elle a été retirée de la plupart de ceux-ci. Les renseignements n'étaient pas chiffrés ou protégés par un mot de passe comme sur le CD envoyé entre les autres ministères provinciaux. Toutefois, la technologie désuète aurait été nécessaire afin de pouvoir accéder aux renseignements disponibles sur la cartouche. Il est peu probable qu'un tiers puisse avoir eu accès aux renseignements contenus dans les cartouches.

Le service de messagerie a informé l'entrepreneur que le colis avait été perdu. La Gendarmerie royale du Canada (GRC) s'est rendue au dernier terminal où la cartouche a été numérisée et croit que la cartouche a été non pas volée, mais perdue.

Pour analyser la gravité de l'atteinte, il est important de souligner que l'on croit que les cartouches sont perdues. De plus, même si ces cartouches contiennent des renseignements personnels, les renseignements sur la santé sont limités aux renseignements sur la facturation dont la nature n'est pas aussi délicate que le seraient des renseignements sur le diagnostic ou des renseignements détaillés sur la santé. Afin d'accéder aux renseignements sur la cartouche, il faut avoir un ordinateur central et une technologie relativement désuète.

La préoccupation, cependant, est la suivante. S'il était possible d'accéder aux renseignements, les cartouches renferment bien le nom, le sexe et le numéro d'assurance-maladie, ce qui permettrait à toute personne intéressée d'utiliser les renseignements pour une usurpation d'identité. L'usurpation d'identité se produit lorsqu'une personne utilise les renseignements vous identifiant personnellement, comme votre nom, votre numéro d'assurance-sociale, ou d'assurance-maladie, ou votre numéro de carte de crédit, sans votre permission, pour commettre une fraude ou d'autres actes

criminels. Selon la Commissaire à la vie privée du Canada les pertes totales reliées à l'usurpation d'identité se chiffrent dans les milliards de dollars par année à travers le monde, ce qui explique pourquoi on y réfère comme étant « le crime du 21^{ème} siècle ». En ayant ces renseignements en main, des criminels peuvent obtenir des cartes de crédit au nom de la victime, qu'ils utiliseront jusqu'à la limite et ne payeront pas, ce qui laissera la victime avec un mauvais dossier de crédit et une facture non réglée. Ils peuvent également essayer d'ouvrir un compte de banque ou de contracter un prêt hypothécaire, selon la quantité de renseignements personnels dont ils disposent.

3.3 Mesures de sécurité en place avant l'incident

Les mesures de sécurité en place au moment de l'incident portaient sur la sécurité physique du centre des données même et n'englobaient pas le processus de transmission des renseignements. Le centre des données qui loge les ordinateurs centraux sur lesquels résident les renseignements se trouve dans un emplacement confiné qui est seulement accessible au personnel autorisé. D'autres dispositifs de sécurité comme des caméras de sécurité disposées à l'intérieur du centre et du périmètre sont en place.

Après que la cartouche quitte le centre des données, la sécurité semble retenir moins d'attention. Les cartouches sont placées dans des enveloppes ordinaires. Elles sont envoyées par service de messagerie et portent le nom du destinataire et celui de l'expéditeur. Aucun système de suivi n'était en place, que ce soit au service de messagerie ou au ministère de la Santé, qui aurait indiqué qu'un colis est arrivé à temps. De plus, aucun ruban-masque inviolable n'a été utilisé.

Comme il est énoncé ci-dessus, les lignes directrices d'interprétation applicables au principe 7 de la LPRP indiquent expressément que les normes exigées « comprennent les dispositifs de protection qui doivent être adoptés quand un organisme public divulgue des renseignements personnels à un tiers ». Les contrats que le ministère de l'Approvisionnement et des Services avait conclus avec son fournisseur X-wave étaient inadéquats en ce qui concerne les garanties contractuelles qui conviendraient, compte tenu de la nature délicate de l'information traitée par le système d'information sur la facturation de l'Assurance-maladie. Notre examen n'a comporté aucun examen de l'architecture de la sécurité du système de facturation même de l'Assurance-maladie, qui est un ancien système, d'après ce que nous avons cru comprendre.

3.4 Politiques et modalités du ministère

En septembre 2007, le gouvernement du Nouveau-Brunswick a approuvé la Politique sur les systèmes de technologie de l'information du gouvernement. Il est indiqué dans le document des normes et des directives ayant trait à la politique que :

L'information du gouvernement est un précieux atout... Pour assurer que l'information peut continuer de servir aux fins pour lesquelles elle a été recueillie, elle doit être protégée contre la divulgation, la modification,

l'utilisation ou la destruction non autorisées. On doit prendre des mesures pour assurer le maintien de sa confidentialité, de sa disponibilité et de son intégrité.

Les normes et les directives reposent sur les pratiques exemplaires et les normes en vigueur dans l'industrie. Elles fournissent les normes pour les mots de passe, l'octroi d'un accès, la sécurité des postes de travail, la sécurité du courrier électronique, etc. Le document ne traite pas du transfert de ces renseignements à l'extérieur de la province.

Lorsque l'atteinte à la vie privée est survenue, il n'y avait, au ministère de la Santé, aucune politique sur la protection des renseignements personnels, aucune politique sur le mode de transmission de ces renseignements ni aucune politique sur les atteintes à la vie privée. Un fonctionnaire au Ministère a admis à nos enquêteurs que ce n'était pas la première fois que des cartouches des données de facturation de l'Assurance-maladie avaient été égarées ainsi. Selon lui, lorsque le Ministère a appris de BC Health que les cartouches n'étaient pas arrivées, la seule mesure qui a été prise selon la pratique établie a été de produire de nouvelles cartouches à l'aide des mêmes renseignements sur la facturation et de les envoyer de la même manière. La culture de l'organisation a établi bien clairement que les factures doivent être réglées. Malheureusement, la protection des renseignements personnels des patients n'a pas bénéficié de la même application zélée.

3.5 Mesures prises par le ministère de la Santé à la suite de l'atteinte

Après que les cadres supérieurs au Ministère ont été informés de l'atteinte, plusieurs mesures ont été prises. Le ministère de la Santé a cessé d'envoyer les renseignements par cartouche et a travaillé avec HIBC à concevoir des protocoles pour transmettre les renseignements par CD chiffré à court terme. Avant l'atteinte, les deux organisations avaient travaillé durant des mois pour changer le processus et remplacer les cartouches par un CD chiffré. Malheureusement, ce processus n'a pas été achevé avant que les cartouches se perdent. Le Ministère a accéléré les pourparlers avec les autres instances pour adopter le protocole de transfert de fichier afin de transmettre les renseignements de ce genre.

En plus de s'affairer à trouver un moyen plus sécurisé de transférer les renseignements, le Ministère s'est concentré sur la notification des parties concernées. Le ministre a donné un avis public de l'atteinte à l'Assemblée législative le 11 décembre 2007. Le même jour, le ministère de la Santé a communiqué avec les personnes concernées par téléphone. Il a envoyé des lettres aux personnes qu'il n'a pas pu joindre par téléphone, le 14 décembre 2007. Des annonces ont été publiées dans les journaux au Nouveau-Brunswick et en Colombie-Britannique. Le Ministère a offert des services de surveillance du crédit à toutes les parties concernées pour une année complète.

L'atteinte a également attiré l'attention du Ministère sur le manque de politiques en place pour traiter cette situation. Après l'atteinte, une politique sur l'atteinte aux données a été élaborée. Le Ministère a entrepris un examen des risques associés à tous les transferts des données. De plus, une analyse du transfert sécurisé des données a été menée en décembre afin de déterminer un processus plus sécurisé pour le transfert intergouvernemental des

données. Une note de service a été envoyée à tous les employés du ministère de la Santé pour les informer que toute atteinte aux renseignements personnels devait être signalée au sous-ministre.

3.6 Constatations

Dispositifs de protection – Les dispositifs en place au moment de l’atteinte n’étaient pas suffisants, compte tenu de la nature délicate des renseignements personnels. Les renseignements ont été transférés dans un format non sécurisé. Plusieurs décisions récentes prises par des commissaires à la vie privée au Canada ont confirmé que, chaque fois que des renseignements personnels quittent l’enceinte de l’établissement physique où ils sont conservés, que ce soit un ordinateur portable, un terminal mobile de poche, un CD ou un autre dispositif portatif, les renseignements doivent être chiffrés. Le meilleur dispositif de protection consiste à élaborer des politiques et des pratiques qui limitent au minimum l’utilisation de tels renseignements à l’extérieur des établissements de soins de santé. Le ministère de la Santé a un rôle de leadership à jouer afin de s’assurer que les régies régionales de la santé et tous les dépositaires de renseignements personnels sur la santé adoptent et appliquent de tels dispositifs de protection minimales. Dans ce contexte, je détermine qu’en ne procédant pas de façon plus rapide pour adopter les méthodes de FTP et les technologies de CD chiffré comme normes provinciales pour le transfert des renseignements sur la facturation réciproque de l’Assurance-maladie, le Ministère s’est retrouvé à tous égards à manquer à ses obligations en vertu du principe 7 de la *Loi sur la protection des renseignements personnels*.

Après l’atteinte, le Ministère a fait une recherche sur les pratiques exemplaires en matière de transfert de données matérielles, dont celles des autres ministères, de la GRC et du Conseil du Trésor (CT) du Canada. Il a indiqué à notre bureau qu’il mettra en œuvre ces dispositifs, dont l’utilisation d’un ruban-masque inviolable et d’un système de suivi de la documentation. De plus, tant avant qu’après l’atteinte, le Ministère a travaillé avec les autres ministères de la Santé, par l’entremise du groupe de travail intergouvernemental, afin d’établir des méthodes plus sécurisées pour transférer les données. À mon avis, ces mesures sont encourageantes, mais insuffisantes.

Comme strict minimum, le Ministère a omis de prendre des dispositifs de protection adéquats afin de s’acquitter de ses obligations en vertu de la LPRP en omettant d’effacer les renseignements de nature délicate de 485 résidents du Nouveau-Brunswick, avant de retourner les cartouches en Colombie-Britannique avec des renseignements supplémentaires sur la facturation concernant les 149 résidents de la Colombie-Britannique qui avaient reçu des services ici. HIBC n’avait plus besoin des renseignements du Nouveau-Brunswick, et l’omission de supprimer l’information de nature délicate de ces cartouches avant de les retourner était négligente.

Documents de politique - Les documents de politique sur la protection des renseignements personnels et la notification d'atteintes font crûment défaut. Le ministère de la Santé traite chaque jour de renseignements personnels et de renseignements personnels sur la santé. Notre enquête a révélé un manque de documents de politique qui traitent de l'importance de protéger les renseignements personnels. Elle a indiqué également un manque de compréhension de la part du personnel au sujet de l'importance de protéger les renseignements personnels. Vu la quantité de renseignements personnels que détient le Ministère de même que l'élaboration de dossiers de santé électroniques, il est important que le ministère de la Santé protège mieux ces renseignements personnels.

Notification d'une atteinte – Cela a pris plus de six semaines avant que les cadres supérieurs au ministère de la Santé soient informés des renseignements manquants. Il faut en attribuer la faute non pas à une personne en particulier, mais plutôt à un manque de politiques et de procédures dans l'organisation. Après l'atteinte, une note de service interne a été envoyée à tous les employés au ministère de la Santé pour indiquer que toute atteinte ou atteinte soupçonnée aux renseignements personnels, comme un ordinateur portable volé ou des colis perdus dans le courrier, doit être signalée immédiatement au sous-ministre. C'est un début louable, cependant, cela ne va tout simplement pas assez loin.

Formation - Dans son discours à l'Assemblée législative, le ministre a déclaré que le Ministère accorde la priorité absolue à la protection des renseignements personnels. « Nous savons que les résidents du Nouveau-Brunswick nous ont confiés la garde de ces renseignements et que nous avons l'obligation de maintenir cette confiance » (trad.). Après avoir été informés des cartouches perdues, les cadres supérieurs du Ministère sont intervenus rapidement pour enquêter sur l'atteinte et aviser les parties concernées. Je n'ai aucun doute que le ministre et les cadres supérieurs n'ont que trop conscience de l'importance de la protection des renseignements personnels. Compte tenu du fait que personne n'a été informé des cartouches perdues avant près d'un mois après leur disparition, je ne suis pas sûr que tous les employés au Ministère soient aussi conscients de l'importance de protéger les renseignements personnels.

4.0 Recommandations

1) Responsabilité – Il est recommandé de créer un poste de chef de la protection des renseignements personnels au ministère de la Santé.

Le ministère de la Santé a besoin d'un chef de la protection des renseignements personnels semblable à l'agent corporatif à la protection de la vie privée à Services Nouveau-Brunswick. Cette personne devrait être un cadre supérieur. Le chef de la protection des renseignements personnels aura pour rôle d'élaborer des principes de protection de la vie privée à l'échelle du ministère, qui comprendraient l'élaboration de politiques, de pratiques et de protocoles; la formation du personnel, une aide à la création de schémas d'acheminement des données, l'examen des évaluations des facteurs relatifs à la vie privée (une analyse des projets afin de cerner les risques qu'ils présentent à la vie privée), l'examen ou la création de calendriers de conservation, la mise à jour des

politiques, des pratiques et des protocoles après la présentation de toute nouvelle loi et l'exécution de vérifications internes de la protection de la vie privée.

En créant ce poste et en lui donnant sa légitimité interne, le Ministère contribuerait beaucoup à s'acquitter de sa responsabilité en vertu du principe 1 de la *Loi sur la protection des renseignements personnels*. Le chef de la protection des renseignements personnels pourrait aider le sous-ministre à se départir de son rôle en tant que personne désignée par la loi qui est responsable du respect par l'organisme public des principes de protection de la vie privée. Il pourrait également faire la liaison entre le Ministère et les régies régionales de la santé, ce qui aiderait à élaborer des politiques et des pratiques de protection de la vie privée entre les organisations.

2) Politique et procédures – Il est recommandé que le ministère de la Santé élabore une politique détaillée de protection de la vie privée et l'incorpore en modalités individuelles. Cette politique devrait être examinée chaque année.

Le ministère de la Santé a besoin d'une politique détaillée de protection de la vie privée pour l'organisation. Avant d'élaborer cette politique, il faudrait que le chef de la protection des renseignements personnels recommandé ci-dessus examine les pratiques actuelles de traitement de l'information et élabore un schéma d'acheminement des données pour déterminer comment l'information est acheminée à l'intérieur et à l'extérieur de l'organisation. Après l'élaboration d'une politique ministérielle de protection de la vie privée, le chef de la protection des renseignements personnels devrait ensuite descendre dans la hiérarchie jusqu'aux postes des employés individuels et des membres d'équipe pour s'assurer que les modalités applicables à ces personnes et équipes incorporent la protection de la vie privée, en particulier la détection et la déclaration des atteintes à la vie privée.

La politique de protection de la vie privée devrait comporter des renvois à l'obligation du ministère de la Santé en vertu de la LPRP et de toute future loi, ainsi que des définitions de renseignements personnels et de renseignements personnels sur la santé, d'atteinte à la vie privée, etc. Elle devrait indiquer les points à l'égard de la responsabilité, et traiter des questions liées à la vie privée des employés et des clauses contractuelles, pour n'en nommer que quelques-uns.

3) Formation– Il est recommandé que le ministère de la Santé offre une formation supplémentaire aux employés relative à la LPRP.

Par l'entremise d'un entrepreneur indépendant, le Bureau des ressources humaines a élaboré un cours en ligne sur la *Loi sur la protection des renseignements personnels*. Ce cours est offert aux employés par la voie du Centre du savoir ILearn, site intranet utilisé pour faciliter l'apprentissage en ligne. Le ministère de la Santé devrait mettre en œuvre des modalités pour faire le suivi des employés qui ont reçu la formation afin de s'assurer que tous les employés, actuels et nouveaux, ont suivi le cours. De plus, le Ministère devrait inclure dans sa formation un suivi auprès des employés afin de déterminer comment la protection des renseignements personnels s'applique à leur poste précis.

4) Notification – Il est recommandé que le projet de loi sur la protection des renseignements personnels sur la santé comprenne une exigence d’aviser le Bureau de l’ombudsman des atteintes.

Le Groupe de travail sur les renseignements personnels sur la santé du Nouveau-Brunswick a recommandé, entre autres, dans son rapport publié en septembre 2007 « que lorsqu’un dépositaire de RPS manque à ses obligations ou lorsqu’une mesure de protection de la vie privée échoue, celui-ci ait à en informer la ou les personnes concernées ainsi que le commissaire à l’information et à la protection de la vie privée ». Dans ce cas en particulier, le Ministère a effectivement avisé les personnes concernées par l’atteinte. Cependant, le Bureau de l’ombudsman a été informé de la situation par le commissaire à l’information et à la protection de la vie privée de la Colombie-Britannique. Il serait bien plus approprié à l’avenir que le dépositaire informe le Bureau de l’ombudsman directement. J’appuie sans réserve la recommandation du groupe de travail voulant que les dépositaires doivent informer l’organisme de surveillance.

En l’espèce, même si notre appel au ministère de la Santé a précédé toute notification officielle à notre bureau, le ministère de la Santé a tout mis en œuvre pour nous tenir au courant de ses mesures et progrès à la suite de l’incident de l’atteinte et a prêté un grand secours durant la présente enquête.

5) Impartition – Il est recommandé que le ministère de la Santé mène un examen de toutes les ententes actuelles avec des fournisseurs de services de gestion de l’information et d’autres fournisseurs responsables de la collecte, du traitement ou de l’utilisation de renseignements personnels sur la santé pour s’assurer que le contrat comprenne des dispositifs de protection adéquats.

Non seulement dans le contexte actuel, mais de plus en plus à mesure que le gouvernement ira de l’avant avec la prestation des applications de l’infomoteur dans la province, le ministère de la Santé traitera de façon provisoire et à long terme avec des fournisseurs de solutions dans le secteur privé, qui auront accès aux renseignements personnels sur la santé sur support électronique, dans le but d’élaborer et de maintenir les systèmes. Il est primordial de limiter au minimum de telles utilisations et d’établir des dispositifs de protection adéquats dans l’élaboration et la mise à l’essai de ces initiatives afin de ne pas poser de risques plus grands aux renseignements personnels sur la santé qu’il ne l’est strictement nécessaire. À long terme, les activités de maintenance des systèmes qui sont imparties, comme cela a été le cas en l’espèce, doivent être assujetties aux obligations et aux dispositions législatives qui sont conformes aux pratiques exemplaires de protection de la vie privée dans le domaine.

6) Prochaines étapes – Le ministère de la Santé doit entreprendre sans tarder l’examen complet de ses pratiques de gestion de l’information avec l’aide d’un expert-conseil de l’extérieur de l’organisation.

Comme il a été énoncé ci-dessus, notre bureau a été invité par le ministre, invitation qu'il a refusée, à mener un examen approfondi de toutes les pratiques de gestion de l'information au ministère de la Santé et à vérifier et à améliorer la protection de la vie privée et leur sécurité. Pour les raisons susmentionnées, il n'est pas possible pour l'ombudsman d'entreprendre un examen de cette portée et de cette nature. Toutefois, il est évident, d'après notre enquête actuelle, qu'une refonte des systèmes s'impose de toute urgence. Il est primordial, à mon avis, d'entreprendre autant de ces activités que possible avant que d'autres projets de l'infrastructure ne soient implantés. Avant de poursuivre l'élaboration du dossier de santé électronique, nous recommandons que tous les systèmes de soutien à l'information au Ministère soient soumis à des évaluations rigoureuses de la menace et des risques externes et des facteurs relatifs à la vie privée.

Par exemple, le Ministère et les experts dont il retiendra les services devraient examiner le récent rapport de la commissaire à l'information et à la protection de la vie privée de l'Ontario à la suite de son examen de la protection de la vie privée et de la sécurité au sein de l'agence ontarienne qui a reçu pour mandat d'aider à l'automatisation des systèmes informatiques pour la santé dans les régions de la santé en Ontario, l'examen de l'initiative « Systèmes intelligents pour la santé ». Le rapport contient 82 recommandations dont la plupart ont maintenant été mises en œuvre par l'Agence des systèmes intelligents pour la santé. Le rapport et son accueil nous donnent une bonne idée du travail qui attend le Nouveau-Brunswick.

Je serai heureux de revenir à cette question pendant que la province mettra au point la demande de propositions et le cadre de référence de l'examen que le Ministère a demandé plus tôt à notre bureau.

5.0 Conclusion

L'atteinte aux renseignements personnels qui est survenue en octobre 2007 a, espérons-le, servi à rappeler de façon importante, sinon pénible, au ministère de la Santé de même qu'à tous les autres ministères que la protection de la vie privée est une question qui mérite toute notre attention. Il ne suffit pas de dire que la protection des renseignements personnels est importante dans l'organisation. Le ministère de la Santé ainsi que les autres ministères doivent s'assurer que la protection des renseignements personnels est un objectif de chaque employé de l'organisation qui traite les renseignements personnels.

Cette enquête a permis de clarifier ce que plusieurs commentateurs ont dit pendant des années. L'adoption de la LPRP comme première loi au Nouveau-Brunswick concernant la protection de la vie privée dans le secteur public, a contribué à mieux sensibiliser la population et à accroître les attentes des citoyens à l'égard de la protection de la vie privée dans leurs rapports avec les pouvoirs publics. Cependant, la LPRP a eu des incidences trop limitées sur la façon dont les pouvoirs publics gèrent les renseignements personnels. Diverses raisons pourraient l'expliquer. Peut-être que la loi n'était pas assez

prescriptive, ou qu'elle était trop vague, peut-être que la formation des employés a été trop limitée, peut-être que des ressources insuffisantes ont été affectées afin d'appliquer la loi de façon adéquate, peut-être que la responsabilité n'a pas été intégrée aux responsabilités courantes des gestionnaires et du personnel ou n'a pas été considérée de façon adéquate dans leurs évaluations du rendement. À bien des égards, nous n'avons pas encore saisi à quel point la tâche de protéger les renseignements personnels à l'ère du cybergouvernement et de la prestation des services en ligne est lourde.

Armés d'un nouveau cadre législatif et de dispositions précises dans le secteur des soins de santé, nous aurons une nouvelle possibilité de nous départir de cette tâche comme il le faut. D'autres provinces le font et sont bien plus avancées sur cette courbe que nous le sommes. Il est temps que le Nouveau-Brunswick rattrape son retard sur le reste du Canada.