

**Lignes directrices relatives à la collecte, à la
conservation, à la transmission et à la
destruction des informations contenues dans
les dossiers de santé électroniques**

Novembre 2009



Canadian Alliance of Physiotherapy Regulators
Alliance canadienne des organismes de réglementation de la physiothérapie

1243 Islington Avenue, Suite 501, Toronto ON M8X 1Y9 t:416-234-8800 f: 416-234-8820 www.alliancept.org

Table des matières

Mot de remerciement	3
Avis aux lecteurs	4
Avant-propos	5
A. Collecte des informations contenues dans les dossiers de santé électroniques.....	6
i. Le consentement du client.....	6
ii. Lois pertinentes et leurs mécanismes de mise en application	6
iii. Normes en vigueur régissant la transmission	7
B. Maintien d'un système de gestion intégrale de dossiers de santé électroniques.....	7
i. Plan de sauvegarde des données	7
ii. Procédures de suppression de données	8
iii. Contrôle de l'accès aux informations	9
iv. Formation du personnel quant aux mesures de sécurité	9
v. Gestion de la configuration des mesures de sécurité.....	9
vi. Procédures visant le dépistage d'incidents.....	10
vii. Contrôle de l'accès physique aux données	10
viii. Formation.....	10
ix. Signalement des infractions.....	11
C. Transmission des données de santé électroniques	11
i. Contenu des transmissions.....	11
ii. Ententes portant sur la transmission des informations.....	11
Bilan et conclusions	12
Ouvrages de référence	13
Annexe A - Lois et règlements qui régissent les informations dans le domaine de la santé (en date du mois de novembre 2009)	14
<i>Loi sur la protection des renseignements personnels</i>	15
Annexe B - Accord de non-divulgation à l'intention des employés/étudiants/bénévoles...	18
Annexe C - Déclaration accompagnant la transmission des données de santé électroniques...	19
Schedule D - Exemple d'un accord couvrant la transmission électronique de données de santé .	20



Mot de remerciement

Le présent document a été conçu et rédigé avec l'apport des organismes de réglementation, des membres de l'Alliance, et celui d'autres partenaires pertinents à travers le Canada. L'Alliance canadienne des organismes de réglementation de la physiothérapie (l'« Alliance ») tient à exprimer ses sincères remerciements aux personnes et aux organismes suivants :

- Les organismes de réglementation de la physiothérapie de la région de l'Atlantique
- Mark Raven-Jackson et Jane Steblecki de la firme Field LLP
- Les organismes membres de l'Alliance
- Les membres du RWFSI (*Regulatory Workgroup on Funding System Issues* - Groupe de travail consacré aux problématiques liées aux méthodes de financement)

Annick deGooyer
Jenneth Swinamer
Moyra Holliday
Dennis Desautels
Carol Puri
Pamela C. Fralick
Joan Ross
Margaret Butler
Dianne Millette



Avis aux lecteurs

Ce document résume les points importants que les organismes de réglementation de la physiothérapie * doivent considérer en fournissant à leurs membres des renseignements sur la collecte, la conservation, la transmission et la destruction des dossiers de santé électroniques.

Les principes régissant la gestion des dossiers de santé électroniques ne sont pas inconnus des physiothérapeutes au Canada. Dans le cadre de leurs juridictions respectives, les physiothérapeutes sont tenus de faire preuve de diligence en collectant, conservant, transmettant et éliminant les dossiers de santé, quelle que soit la méthode employée pour leur sauvegarde. Toutefois, en raison des progrès technologiques récents et des risques associés à la transmission des données par voie électronique, les physiothérapeutes doivent prendre les mesures qui s'imposent quant à la gestion de la confidentialité et du consentement de la clientèle.

Les physiothérapeutes doivent tenir compte des rapports établis entre la gestion des dossiers et des projets de loi sur la protection de la vie privée, et se renseigner au sujet d'initiatives comme le projet NeCST de l'Institut canadien de l'information sur la santé, visant l'établissement de normes régissant la transmission électronique des dossiers de santé. Des initiatives des gouvernements fédéral et provincial énonçant les obligations légales quant à la protection de la vie privée, influent sur la façon dont les informations électroniques sont recueillies, conservées et transmises. Des lois fédérales comme la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ont une grande portée sur toute activité commerciale impliquant la collecte, l'usage et la transmission des informations personnelles. Veuillez consulter l'*annexe A* de ce document qui énumère les lois en vigueur dans chacune des juridictions.

Le domaine des dossiers de santé électroniques connaît un formidable essor. C'est pourquoi, ce document doit être considéré comme un travail en cours. L'implication croissante des physiothérapeutes dans la gestion des dossiers de santé électroniques, y compris les systèmes de facturation électroniques, exigera une mise à jour ultérieure de ce document.

Dans le cadre de toutes les juridictions, il incombe aux physiothérapeutes enregistrés/inscrits de se familiariser avec les lois en vigueur et de leur impact sur l'exercice sécuritaire, efficace et éthique de leur profession. Celles-ci comprennent mais ne se limitent pas à la conformité aux normes de réglementation et autres dispositions (p.ex. : les lois gouvernant les centres hospitaliers, les indemnités pour accidents de travail et la confidentialité des renseignements sur la santé).

Tous les physiothérapeutes, cliniques de physiothérapie et autres organismes responsables de la collecte d'informations sur la santé, devraient consulter leurs services juridiques pour connaître :

- a. leurs obligations en vertu de la loi quant à la collecte, à la conservation, à l'usage et à la transmission des dossiers de santé électroniques;
- b. les amendes et pénalités résultant d'une violation des lois;
- c. les projets de loi au niveau provincial qui pourraient avoir un impact sur les techniques employées par les physiothérapeutes quant à la gestion des dossiers de santé électroniques.

Nous encourageons les physiothérapeutes désirant obtenir de plus amples renseignements au sujet de la conservation et de la transmission des dossiers de santé électroniques, de communiquer avec l'organisme de réglementation de la physiothérapie de leur province/territoire.

* Physiothérapie et les termes qui s'y rapportent sont des marques officielles utilisées avec permission.



Avant-propos

En raison de récents progrès technologiques, de nombreux physiothérapeutes utilisent des systèmes de gestion de dossiers de santé électroniques dans le cadre de la prestation de leurs services. Ce faisant, ils facilitent l'entreposage et la récupération de ces documents. Le 28 novembre 2002, le rapport Romanow promeut auprès des professionnels de la santé au Canada l'utilisation et la conservation des dossiers de santé électroniques. Ils pourraient ainsi :

- accéder facilement à l'histoire médicale du client;
- documenter clairement et précisément les réponses du client au traitement;
- obtenir des dossiers de santé exacts, lisibles et bien organisés;
- avoir en main des dossiers électroniques protégeant mieux la confidentialité que ceux en papier.

Les technologies relatives à Internet et à la transmission de courriels ont également progressé de façon à faciliter l'envoi par les physiothérapeutes des informations¹ contenues dans les dossiers de santé électroniques aux agences et organismes de financement.

Aujourd'hui, l'on cherche à accroître les communications électroniques entre les agences et les organismes de financement et les physiothérapeutes aux fins suivantes :

- réduire les heures consacrées au travail administratif;
- simplifier les procédures de facturation;
- cibler le traitement associé au coût le plus rentable;
- évaluer le bien-fondé des demandes d'indemnité.

Le présent document adresse les sujets suivants :

- A. La collecte des dossiers de santé électroniques :
 - i. Le consentement du client;
 - ii. Lois pertinentes et leurs mécanismes de mise en application;
 - iii. Normes en vigueur régissant la transmission.

- B. Le maintien d'un système de gestion intégrale des dossiers de santé électroniques :
 - i. Plan de sauvegarde des données;
 - ii. Procédures de suppression des données;
 - iii. Contrôle de l'accès aux informations;
 - iv. Formation du personnel quant aux mesures de sécurité;
 - v. Gestion de la configuration des mesures de sécurité;
 - vi. Procédure de gestion d'incidents affectant la sécurité;
 - vii. Contrôle de l'accès physique aux données;
 - viii. Formation;
 - ix. Signalement des infractions.

- C. La transmission des informations contenues dans les dossiers de santé électroniques
 - i. Contenu des dossiers transmis;
 - ii. Ententes régissant la transmission.

¹ En règle générale, les informations de santé constituent un dossier sur les diagnostics et les traitements permettant d'identifier la personne ayant reçu des services de physiothérapie. Un tel dossier devrait inclure les informations électroniques conservées dans une banque de données ou sur un serveur.



A. La collecte des informations contenues dans les dossiers de santé électroniques

i. Le consentement du client

Les physiothérapeutes sont habitués à recueillir auprès de leurs clients des données de santé confidentielles et de les traiter avec tout le soin qui s'impose. Toutefois, la conservation et la transmission électroniques des données de santé, comportent des risques additionnels qui devront être communiqués au client afin d'obtenir de celui-ci un consentement éclairé au traitement.

Toute discussion éclairée entre un physiothérapeute et son client devrait :

- aborder les méthodes employées pour la création et la conservation d'un dossier de santé électronique;
- avoir lieu lorsque le client se présente pour son premier traitement;
- être l'occasion de fournir au client un dépliant expliquant les mesures de sécurité mises en œuvre;
- être résumée par écrit, le document devant être signé par le client.

À cet égard, le physiothérapeute devrait penser à inclure dans le formulaire de consentement un paragraphe traitant de la conservation et de la transmission des dossiers de santé électroniques. Un tel paragraphe pourrait se lire comme suit :

« Je consens à ce que (nom du physiothérapeute) gère mon dossier de santé en un format électronique et je comprends que celui-ci puisse être transmis à (catégories générales ou noms spécifiques d'agences de financement, organisations ou autres prestataires des soins de santé) dans le cadre de mon traitement. Les risques et avantages découlant de la conservation et de la transmission de mon dossier de santé électronique m'ont été expliqués. »

Nous tenons à souligner qu'un formulaire de consentement standard ne pourra jamais remplacer un entretien détaillé et ponctuel avec le client. En fait, le formulaire ne devrait servir qu'à établir que l'entretien ait bel et bien eu lieu.

De plus, nous devons reconnaître qu'un client a le droit de refuser son consentement à la conservation de son dossier de santé sous format électronique et à sa transmission par le biais du réseau Internet. Advenant un tel refus, des pourparlers devront être entamés avec les agences ou organismes de financement pour trouver les mesures en place pouvant accommoder les volontés du client.

Finalement, nous devons tenir compte des attentes réelles du client lorsque celui-ci nous donne son consentement comprenant, entre autres, la collecte et la conservation justifiées et nécessaires des données de santé en format électronique. Le principe sous-tendant la collecte, l'utilisation et la transmission des données de santé, énonce que seules les informations essentielles permettant au physiothérapeute ou à leur destinataire, selon le cas, à réaliser leurs objectifs exprimés, peuvent être collectées, utilisées ou transmises.

ii. Lois pertinentes et leurs mécanismes de mise en application

Au cours des dernières années, plusieurs provinces ont adopté des lois sur les dossiers de santé électroniques afin de combler un manquement quant à la réglementation des réseaux de gestion de dossiers de santé électroniques au Canada. En cherchant à introduire rapidement ces lois, les provinces ont élaboré des modèles législatifs différents.

Vu l'évolution continue dans ce domaine, la collecte, l'utilisation et la transmission des dossiers de santé électroniques, à une échelle nationale, soulèveront encore des questionnements à court terme.

Présentement, un mouvement pancanadien visant à modifier et à harmoniser les lois sur les dossiers de



santé électroniques, et une volonté à créer une base de données de santé électroniques nationale (tel que promu à la recommandation 12 du rapport Romanow) feront progresser ce dossier.

Toutes les lois sur la gestion des données de santé s'accordent quant aux pénalités et aux amendes pouvant être appliquées pour les infractions commises par les prestataires de soins de santé. Le montant des amendes peut être élevé et les pénalités encourues peuvent avoir un impact important sur l'exercice de sa profession par le physiothérapeute.

iii. Normes en vigueur régissant la transmission

Même si les autres professionnels de la santé font usage depuis plusieurs années d'Internet pour acheminer les dossiers de santé, les physiothérapeutes ont à peine commencé à les imiter. Les dentistes et pharmaciens, notamment, font emploi depuis longtemps de systèmes de facturation électronique en hyperlien avec les données de santé des patients. Ainsi, les normes régissant la transmission de données ont évolué et les physiothérapeutes collaborent dorénavant avec d'autres prestataires de soins de santé en vue de l'adoption de normes internationales reconnues pour la transmission des dossiers de santé.

B. Le maintien d'un système de gestion intégrale de dossiers de santé électroniques

Tout système régissant les informations contenues dans les dossiers de santé électroniques devrait inclure :

- a. un matériel informatique et un système d'exploitation fournissant les suivants : des liens longitudinaux et temporels vers d'autres dossiers ou systèmes d'information du dossier du patient; un accès autorisé continu; un soutien en simultané à d'autres interfaces d'utilisateur; un accès à des sources d'informations locales ou éloignées;
- b. un logiciel de gestion de dossiers effectuant les tâches suivantes : protéger la confidentialité et procurer des pistes de vérification; fournir des listes de problèmes; effectuer la sauvegarde de dossiers détaillant le rationnel des raisonnements cliniques; faciliter la résolution de problématiques cliniques; supporter la saisie de données par les prestataires de soins de santé et aider ceux-ci à évaluer et à gérer les coûts pour améliorer la qualité des soins;
- c. un contenu pouvant évaluer le statut de santé et le niveau fonctionnel des clients tout en procurant la polyvalence requise pour soutenir les besoins changeants de la pratique.

Dès la mise en œuvre d'un système de gestion des dossiers de santé électroniques, il faut veiller à l'intégrité des données et les protéger contre toute possibilité d'altération, d'accès non autorisé ou de purge involontaire. La section suivante se veut un résumé des politiques et procédures devant être conservées par écrit et mises en œuvre afin d'assurer une gestion prudente.

i. Plan de sauvegarde des données

Le physiothérapeute, de même que la clinique ou centre de santé où il travaille, doivent avoir un accès continu aux données de santé électroniques afin de fournir aux clients des soins selon les normes. Comme ces informations pourraient devenir inaccessibles en raison d'une altération de données, ou encore, d'un incendie, leur sauvegarde quotidienne devient une nécessité absolue pour éviter toute perte.

Toute politique sur la sauvegarde des données devrait inclure les renseignements suivants :

- a. le nom du coordonnateur responsable du plan de sauvegarde de données et de l'archivage des dossiers;



- b. la ou les méthodes employées pour effectuer la sauvegarde des données ainsi que la liste de vérification des procédures mises en œuvre;
- c. la fréquence des sauvegardes;
- d. l'emplacement du site où les données sont sauvegardées;
- e. l'emplacement hors site où les données sont sauvegardées;
- f. la nature des données devant être (généralement) sauvegardées.

Il incombe aux physiothérapeutes de choisir les données de santé devant être sauvegardées. Ce choix s'exerce en fonction des informations requises pour être en conformité avec les normes de réglementation ou lois.

Les physiothérapeutes devront effectuer une vérification régulière de leurs données sauvegardées afin d'être en mesure de les remplacer advenant leur corruption ou purge et ce, sans compromettre la prestation des soins aux clients.

Il est conseillé de sauvegarder *toutes* les données de santé se trouvant sur le disque dur du système informatique. On pourra ainsi :

- a. optimiser au maximum la sécurité des données;
- b. restaurer en une étape et au complet toutes les données perdues;
- c. faire restaurer automatiquement les données durant les heures de fermeture de bureau.

Cependant, il faudra tenir compte à plus long terme des exigences techniques quant à la lecture des fichiers de sauvegarde de données. Les mises à niveau de logiciels et leur disponibilité pourraient rendre le repérage de données difficile et engager des coûts importants au cours de périodes de sauvegarde prolongées.

Ainsi, la mise en œuvre de technologies axées sur la sauvegarde des données serait coûteuse et même peu réaliste pour les petites cliniques de physiothérapie. Une clinique ne devrait adopter un système de gestion de dossiers électroniques que si elle possède les ressources requises pour le soutien technique, procédures de sauvegarde adéquates incluses.

ii. Procédures de suppression de données

Les physiothérapeutes doivent avoir mis en place des politiques et procédures bien documentées selon celles qui régissent la conservation des dossiers papier et leur élimination confidentielle et sécuritaire. Celles-ci doivent rencontrer les normes minimales fixées par l'organisme de réglementation de la physiothérapie et par les lois en vigueur.

Le même raisonnement s'applique aux dossiers de santé électroniques. Ainsi, les politiques et procédures courantes devront être modifiées de façon à ce que la suppression des informations de santé contenues dans une base de données électronique se fasse en conformité aux lois en vigueur sur la protection de la vie privée.

Les physiothérapeutes doivent s'assurer que le système de gestion supprime bel et bien les données de santé électroniques et ne les « estampille » pas seulement comme supprimées. Il faut savoir que les données « estampillées » comme supprimées, ne signifie pas pour autant qu'elles ont été purgées du système; en effet, le système de gestion de la base de données peut tout simplement écraser les données de santé électroniques pour faire de la place dans la mémoire.

Si le physiothérapeute veut effectuer une mise à niveau du système de gestion de la base de données, ou encore le remplacer, il est essentiel qu'il fasse purger et reformater le disque dur. Si le disque dur doit être remplacé parce qu'il est endommagé, le physiothérapeute doit veiller à ce qu'il soit détruit. Les firmes de recyclage de systèmes informatiques peuvent offrir ce service.



iii. Contrôle de l'accès aux informations

Les physiothérapeutes doivent identifier les personnes qui, dans leur clinique, pourraient avoir accès aux dossiers de santé électroniques et les modifier. Le niveau d'accès est établi en fonction de la nature de confidentialité des informations. En fait, le physiothérapeute est ultimement responsable des personnes et employés qui ont accès aux dossiers de santé électroniques. C'est pourquoi il leur faut adopter des politiques très précises qui adresseront, entre autres, l'accès aux informations, les procédures de vérification et le permis d'accès.

Tout accès aux dossiers de santé électroniques par le biais d'un terminal doit être contrôlé au moyen d'un mot de passe protégé et personnalisé ou de mesures de sécurité physiques. Un utilisateur ne devrait jamais quitter son poste de travail s'il a ouvert une session, car les informations seraient alors non sécurisées. L'identité de l'utilisateur devrait être confirmée par un jeton d'identification unique comme une bande magnétique ou un mot de passe. Il incombe aux utilisateurs de veiller à la confidentialité de leur mot de passe; de plus, l'adoption d'une politique exigeant la modification régulière des mots de passe est essentielle.

Les physiothérapeutes doivent réévaluer continuellement les privilèges d'accès et purger du système les mots de passe des utilisateurs qui ne doivent plus avoir accès aux informations. En outre, les physiothérapeutes doivent être en mesure de dépister tout accès non autorisé ou toute tentative d'accès au moyen d'un fichier de vérification fournissant une preuve d'infraction ou de mauvais usage du système informatique. L'accès inapproprié de renseignements confidentiels devrait être considéré par tout employeur comme motif de congédiement.

iv. Formation du personnel quant aux mesures de sécurité

Le physiothérapeute doit s'assurer de la gestion des dossiers de santé électroniques par un personnel autorisé et compétent.

Ainsi, selon l'importance de la pratique du physiothérapeute, l'embauche d'un employé à temps complet affecté au service des technologies de l'information (TI) peut s'avérer nécessaire. La gestion de la base de données pourrait être faite par cette personne, ou encore, par le biais d'un contrat de service avec une firme TI, de préférence celle qui a effectué la mise en place du système informatique.

Tous les utilisateurs du système devraient recevoir la formation nécessaire pour assurer la sécurité des dossiers de santé électroniques. Une telle formation serait continue et détaillerait les politiques sur la confidentialité et les procédures sur l'exercice de la physiothérapie. En outre, tout le personnel, y compris les fournisseurs de services TI, devraient signer un accord de confidentialité semblable à celui se trouvant à l'annexe B.

v. Gestion de la configuration des mesures de sécurité

Il incombe au physiothérapeute d'assurer l'actualité des dossiers électroniques en effectuant la mise à jour des systèmes informatiques et des logiciels et en faisant faire l'entretien. Les dispositifs de sécurité doivent être évalués régulièrement; en voici quelques-uns que le physiothérapeute peut utiliser :

- Les virus peuvent corrompre les données et compromettre la sécurité des systèmes informatiques. La mise à niveau régulière des logiciels antivirus est essentielle, car les virus peuvent muter et évoluer au fil du temps. Une mise à niveau immédiate des logiciels antivirus s'avère nécessaire lorsque des nouveaux virus sont détectés et que ceux-ci menacent l'intégrité des systèmes informatiques.
- Tout système connecté en permanence au réseau Internet doit être muni d'un coupe-feu. Ce logiciel bloque l'accès d'un ordinateur à Internet; sa capacité de protection couvre les communications



Internet entrantes et sortantes, et rien ne peut passer sauf sur autorisation expresse du physiothérapeute.

- Si le physiothérapeute utilise un réseau sans fil ou un réseau privé virtuel (RPV), les informations doivent être cryptées. Le cryptage convertit les données en cryptogrammes, les rendant non lisibles par les personnes non autorisées à les accéder. Le décryptage reconvertit les données en leur format d'origine afin des les rendre lisibles.

vi. Procédures visant le dépistage d'incidents

Des politiques et procédures aux fins de vérification des transmissions et réceptions des données de santé doivent être mises en place. Lorsque la confidentialité des données est compromise lors de leur transmission, il faut en déterminer la cause et mettre en œuvre un processus de gestion du risque pour éviter toute répétition ultérieure de la problématique.

Les physiothérapeutes peuvent faire appel à des logiciels de vérification et de dépistage qui servent de journal électronique pouvant surveiller tout usage du système informatique. Par exemple, un employé peut être autorisé à accéder à une partie du système de fichiers électroniques, comme la tarification. Toutefois, le même employé peut ne pas être autorisé à accéder les informations de santé électroniques. Si celui-ci tente d'accéder à une section qui ne lui est pas autorisée en saisissant des mots de passe, ses activités seront enregistrées par la piste de vérification. Les pistes de vérification sont également employées pour enquêter sur les crimes informatiques : les enquêteurs n'ont qu'à « suivre » la piste laissée par l'intrus pour exposer son identité.

vii. Contrôle de l'accès physique aux données

Les mots de passe et les cartes d'accès à bande magnétique ne sont d'aucune utilité si les postes de travail permettent la lecture par un tiers des informations de santé affichées à l'écran de l'ordinateur. Les consoles d'ordinateur et, tout particulièrement les portables, doivent demeurer en un lieu sûr (pièces fermées à clef ou attachés au moyen de câbles de sécurité), pour empêcher leur vol et celui des informations de santé électroniques qu'ils contiennent. Il faut également s'assurer que les employés évitent de mettre en fonction l'option « mémoriser mon mot de passe » inclus avec les ordinateurs de bureau et les portables; les consoles d'ordinateur doivent, en outre, être verrouillées lorsque les employés quittent leur bureau pour une durée prolongée. Les appareils de type « Blackberry » et « iPhone » devraient également faire l'objet de mesures de sécurité rigoureuses, dont le verrouillage, lorsqu'ils demeurent inactifs pendant 15 minutes ou plus (tel que suggéré par les administrateurs de systèmes TI). Ceci minimisera tout risque d'accès non autorisé advenant leur perte. De plus, il est important de souligner que les accessoires informatiques externes ou amovibles tels que les clés et les cartes flash ne devraient contenir que le minimum d'informations nécessaires et être protégés par un mot de passe; une fois les informations transférées ou utilisées, elles devraient être purgées. La sécurité des appareils et accessoires doit être maintenue en tout temps durant leur transport en ne les laissant jamais sans surveillance, à moins qu'ils ne soient rangés en un lieu sûr.

Des politiques et procédures doivent être en place afin de fournir un environnement sécuritaire où l'on peut gérer et conserver un système de dossiers de santé électroniques.²

viii. Formation

Les physiothérapeutes et leurs employés doivent être sensibilisés à l'importance de la saisie exacte des données de santé électroniques : des bulletins et notes de service concernant la transmission sécuritaire de ces données devraient être émis régulièrement. Les fournisseurs de systèmes informatiques

² La *Information and Privacy Commission* de l'Alberta a fait une déclaration au sujet d'un vol d'ordinateurs contenant des informations de santé électronique chez un établissement qui n'avait pas mis en place les politiques et procédures appropriées (rapports d'enquête n° H0054 et H0056)



organisent volontiers des ateliers dans le cadre d'un contrat de service ou dans celui du service après-vente.

ix. Signalement des infractions

Les physiothérapeutes, employés et autres personnes utilisant les données de santé électroniques devraient se familiariser avec une politique de signalement et de gestion des infractions à la protection de la vie privée, mise en œuvre auparavant. Plusieurs lois exigent le signalement obligatoire de toute infraction. Dans tous les cas, un processus devrait être adopté pour minimiser les risques d'infraction et empêcher leur récurrence.

C. La transmission des données de santé électroniques

La transmission des données de santé électroniques par le biais du courriel ou du réseau Internet enlève au physiothérapeute un certain niveau de contrôle. Ainsi, les physiothérapeutes partagent la responsabilité avec les tiers de conserver la sécurité et l'intégrité des informations contenues dans les dossiers de santé électroniques. Les physiothérapeutes devront faire preuve de diligence en déterminant si le récipiendaire des informations a adopté les normes nécessaires pour assurer le maintien de la confidentialité. Tel que mentionné précédemment, des travaux continus sont effectués à l'échelle nationale pour établir des normes de transmission appropriées.

L'accès inapproprié aux informations par les tiers demeure la problématique principale liée à la transmission des données contenues dans les dossiers de santé électroniques. De nombreux organismes avec des politiques d'emploi diverses, peuvent être les récipiendaires d'informations contenues dans les dossiers de santé électroniques; ainsi, les physiothérapeutes devront faire preuve de vigilance en transmettant ou divulguant ces informations.

Les courriels, la sécurité du réseau Internet, les RPV et l'encryptage, utilisés pour les transactions financières, ont réalisé de formidables progrès et sont généralement adéquats pour la transmission et la protection des informations contenues dans les dossiers de santé électroniques. Vu que seule une copie des dossiers est envoyée, le problème de la corruption des données ou de leur purge involontaire durant leur transmission ne se pose pas.

i. Le contenu des transmissions

Le credo principal régissant la divulgation des données contenues dans les dossiers de santé électroniques veut que le physiothérapeute ne communique que le strict minimum d'informations requises aux fins prévues, que ce soit à l'intention d'une agence de financement ou d'un autre prestataire de soins de santé. Ainsi, en cas de bris de la confidentialité, on pourra en réduire la portée.

Toute transmission d'informations contenues dans les dossiers de santé électroniques par courriel ou Internet devrait inclure un énoncé semblable à celui donné en exemple à l'*annexe C*.

ii. Ententes portant sur la transmission des informations

Une entente portant sur la transmission des informations contenues dans les dossiers de santé électroniques, assure que l'agence de financement ou le prestataire de soins de santé à qui ces informations sont destinées, respecte les normes établies par le physiothérapeute. Une telle entente est un contrat conclu entre le physiothérapeute et le récipiendaire des informations, qui protège le physiothérapeute si le récipiendaire brise le lien de confidentialité.



Une entente solide portant sur la transmission des informations, dont un exemple est donné à l'*annexe D*, assure que l'organisme recevant les informations (ainsi que ses employés) mette en œuvre et respecte les politiques en vigueur tout en fournissant au physiothérapeute une immunité advenant un bris de confidentialité. La transmission des informations peut être effectuée par un tiers (par exemple un fournisseur ou gestionnaire de données) et une entente couvrant la transmission devrait inclure les obligations du récipiendaire.

Bilan et conclusions

La qualité des soins et la pratique du physiothérapeute ne peuvent que bénéficier de la mise en œuvre d'un système de dossiers de santé électroniques. La transmission des informations contenues dans ces dossiers facilite les transactions physiothérapeute/agence de financement. Tout usage d'un système de dossiers de santé électroniques exige une planification méticuleuse et l'adoption de politiques et de procédures protégeant ainsi le physiothérapeute, ce dernier étant ultimement responsable du maintien de la confidentialité.



Ouvrages de référence

1. Andrews G; Wilkins GE, « Privacy and the computerized medical record » *Med J Aust* 1992 Aug 17;157(4):223-5.
2. Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada* (November 2002) Commissioner R. Romanow, Q.C.
3. Computer-Based Patient Record Institute, Section 5.2 – « Complying with Consent, Inspection, and Disclosure Requirements »,
4. Lamberg, L., « Confidentiality and privacy of electronic medical records: Psychiatrists explore risks of the “information age » *JAMA* 2001 Jun 27; 285(24):3075-6.
5. Lusk R, « Update on the electronic medical record » *Otolaryngol Clin North Am* 2002 Dec; 35(6):1223-36.
6. Meyers JS, « Electronic medical records: 10 Questions I Didn't Know To Ask » *Fam Pract Manag* 2001 Mar;8(3):29-32.
7. « Model Code for the Protection of Personal Information » <http://laws.justice.gc.ca/en/P-8.6/91270.html#rid-91272>
8. Roberts, J; Decter SR; Nagel D, « Confidentiality and Electronic Medical Records » *Ann Intern Med* 1998 March 15; 128(6):510-1.
9. Shoenberg, R; Safran C, « Internet based repository of medical records that retains patient confidentiality » *BMJ* 2000 Nov 11; 321(7270): 1199-203.



Annexe A – Lois et règlements qui régissent les informations dans le domaine de la santé (en date du mois de novembre 2009)

JURIDICTION PROVINCIALE/ TERRITORIALE ET PORTÉE	TYPE	TITRE	CITATION	LIEN
Niveau fédéral				
Certains secteurs privés et publics. S'applique aux organisations privées régies par les lois fédérales ainsi qu'aux informations de santé recueillies, utilisées et divulguées dans le cadre d'activités commerciales transfrontalières, entre les provinces et dans les limites territoriales d'une province n'ayant pas adopté une législation « substantivement similaire ».	Loi	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)</i>	LC 2000, c. 5	http://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html
Alberta				
Applicable principalement au secteur public – couvrira bientôt les secteurs publics et privés	Loi	<i>Health Information Act</i>	R.S.A. 2000, c. H-5	http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest/rsa-2000-c-h-5.html
Applicable principalement au secteur public – couvrira bientôt les secteurs publics et privés	Règlement	<i>Designation Regulation (under the Health Information Act)</i>	Alta. Reg. 69/2001	http://www.canlii.org/en/ab/laws/regu/alta-reg-69-2001/latest/alta-reg-69-2001.html
Applicable principalement au secteur public – couvrira bientôt les secteurs publics et privés	Règlement	<i>Health Information Regulation (under the Health Information Act)</i>	Alta. Reg. 70/2001	http://www.canlii.org/en/ab/laws/regu/alta-reg-70-2001/latest/alta-reg-70-2001.html
Secteur privé Avis : Déclaré « substantivement similaire » à la LPRPDE	Loi	<i>Personal Information Protection Act</i>	S.A. 2003, c. P-6.5	www.canlii.org/ab/laws/stat/p-6.5/20060718/whole.html
Secteur privé Avis : Déclaré « substantivement similaire » à la LPRPDE	Règlement	<i>Personal Information Protection Act Regulation (under the Personal Information Protection Act)</i>	Alta. Reg. 366/2003	http://www.canlii.org/en/ab/laws/regu/alta-reg-366-2003/latest/alta-reg-366-2003.html
Colombie-Britannique				
Certains secteurs privés et publics	Loi	<i>E-Health (Personal Health Information Access and Protection of Privacy) Act</i>	S.B.C. 2008, c. 38	http://www.canlii.org/en/bc/laws/stat/sbc-2008-c-38/latest/sbc-2008-c-38.html



Certains secteurs privés et publics	Règlement	<i>Disclosure Directive Regulation (under E-Health (Personal Health Information Access and Protection of Privacy) Act)</i>	B.C. Reg. 172/2009	http://www.canlii.org/en/bc/laws/regu/bc-reg-172-2009/latest/bc-reg-172-2009.html
Certains secteurs privés et publics Avis : Déclaré « substantivement similaire » à la LPRPDE	Loi	<i>Personal Information Protection Act</i>	S.B.C. 2003, c. 63	http://www.canlii.org/en/bc/laws/stat/sbc-2003-c-63/latest/sbc-2003-c-63.html
Certains secteurs privés et publics Avis : Déclaré « substantivement similaire » à la LPRPDE	Règlement	<i>Personal Information Protection Act Regulations (under Personal Information Protection Act)</i>	B.C. Reg. 473/2003	http://www.canlii.org/en/bc/laws/regu/bc-reg-473-2003/latest/bc-reg-473-2003.html
Manitoba				
Certains secteurs privés et publics	Loi	<i>Loi sur les renseignements médicaux personnels</i>	C.P.L.M. c. P33.5	http://www.canlii.org/fr/m b/legis/lois/cplm-c-p33.5/derniere/cplm-c-p33.5.html
Certains secteurs privés et publiques	Règlement	<i>Règlement sur les renseignements médicaux personnels (sous la Loi sur les renseignements médicaux personnels)</i>	Règl. du Man. 245/97	http://www.canlii.org/fr/m b/legis/regl/regl-du-man-245-97/derniere/regl-du-man-245-97.html
Secteur public	Loi	<i>Loi sur l'accès à l'information et la protection de la vie privée</i>	C.P.L.M. c. F175	http://www.canlii.org/fr/m b/legis/lois/cplm-c-f175/derniere/cplm-c-f175.html
Secteur public	Règlement	<i>Règlement sur l'accès à l'information et à la protection de la vie privée (sous la Loi sur l'accès à l'information et à la protection de la vie privée)</i>	Règl. du Man. 64/98	http://www.canlii.org/fr/m b/legis/regl/regl-du-man-64-98/derniere/regl-du-man-64-98.html
Nouveau-Brunswick				
Secteur public	Loi	<i>Loi sur la protection des renseignements personnels</i>	L.N.-B. 1998, c. P-19.1	http://www.canlii.org/fr/n b/legis/lois/l n-b-1998-c-p-19.1/derniere/l n-b-1998-c-p-19.1.html
Secteur public	Règlement	<i>Règlement général (sous la Loi sur la protection des renseignements personnels)</i>	Règl. du N.-B. 2001-14	http://www.canlii.org/fr/n b/legis/regl/regl-du-n-b-2001-14/derniere/regl-du-n-b-2001-14.html
Terre-Neuve-et-Labrador				
Certains secteurs privés et publics	Loi (pas encore en vigueur)	<i>Personal Health Information Act</i>	S.N.L. 2008, c. P-7.01	http://www.canlii.org/en/nl/laws/stat/snl-2008-c-p-7.01/latest/snl-2008-c-p-7.01.html



Secteur public	Loi	<i>Access to Information and Protection of Privacy Act</i>	S.N.L. 2002, c. A-1.1	http://www.canlii.org/en/nl/laws/stat/snl-2002-c-a-1.1/latest/snl-2002-c-a-1.1.html
Secteur public	Règlement	<i>Access to Information Regulations (under the Access to Information and Protection of Privacy Act)</i>	N.L.R. 11/07	http://www.canlii.org/en/nl/laws/regu/nlr-11-07/latest/nlr-11-07.html
Territoires du Nord-Ouest				
Secteur public	Loi	<i>Loi sur l'accès à l'information et à la protection de la vie privée</i>	L.T.N.-O. 1994, c. 20	http://www.canlii.org/fr/nt/legis/lois/ltn-o-1994-c-20/derniere/ltn-o-1994-c-20.html
Secteur public	Règlement	<i>Règlement sur l'accès à l'information et à la protection de la vie privée (sous la Loi sur l'accès à l'information et à la protection de la vie privée)</i>	Règl. des T.N.-O. 206-96	http://www.canlii.org/fr/nt/legis/regl/regl-des-tn-o-206-96/derniere/regl-des-tn-o-206-96.html
Nouvelle-Écosse				
Certains secteurs privés et publics	Projet de loi	<i>Personal Health Information Act</i>	Projet de loi 64, première lecture : le 4 novembre 2009	http://www.gov.ns.ca/legislature/legc/bills/61st_1st/1st_read/b064.htm
Certains secteurs privés et publics	Loi	<i>Freedom of Information and Protection of Privacy Act</i>	S.N.S. 1993, c. 5	http://www.canlii.org/en/ns/laws/stat/sns-1993-c-5/latest/sns-1993-c-5.html
Secteur public	Règlement	<i>Freedom of Information and Protection of Privacy Regulations (under Freedom of Information and Protection of Privacy Act)</i>	N.S. Reg. 105/94	http://www.canlii.org/en/ns/laws/regu/ns-reg-105-94/latest/ns-reg-105-94.html
Secteur public	Règlement	<i>Regulations Amending the Schedule to the Act Listing Public Bodies (under Freedom of Information and Protection of Privacy Act)</i>	N.S. Reg. 205/2009	http://www.canlii.org/en/ns/laws/regu/ns-reg-205-2009/latest/ns-reg-205-2009.html
Nunavut				
Secteur public	Loi	<i>Loi sur l'accès à l'information et à la protection de la vie privée</i>	L.T.N.-O (Nu.) 1994, c. 20	http://www.canlii.org/fr/nu/legis/lois/ltn-o-nu-1994-c-20/derniere/ltn-o-nu-1994-c-20.html
Secteur public	Règlement	<i>Règlement sur l'accès à l'information et à la protection de la vie privée (sous la Loi sur l'accès à l'information et à la protection de la vie privée)</i>	Règl. T.N.-O. (Nu.) 206-96	http://www.canlii.org/fr/nu/legis/regl/regl-tn-o-nu-206-96/derniere/regl-tn-o-nu-206-96.html
Ontario				
Certains secteurs privés et publics	Loi	<i>Loi de 2004 sur la protection des renseignements</i>	L.O. 2004, c. 3, ann. A	http://www.canlii.org/fr/on/legis/lois/lo-2004-c-3-



Avis : Déclaré « substantivement similaire » à la LPRPDE		<i>personnels sur la santé</i>		ann-a/derniere/lo-2004-c-3-ann-a.html
Certains secteurs privés et publics Avis : Déclaré « substantivement similaire » à la LPRPDE	Règlement	<i>Dispositions générales (sous la Loi de 2004 sur la protection des renseignements personnels sur la santé</i>	Règl. de l'Ont. 329/04	http://www.canlii.org/fr/on/legis/regl/regl-de-lont-329-04/derniere/regl-de-lont-329-04.html
Île-du-Prince-Édouard				
Secteur public	Loi	<i>Freedom of Information and Protection of Privacy Act</i>	R.S.P.E.I. 1988, c. F- 15.01	http://www.canlii.org/en/pe/laws/stat/rspei-1988-c-f-15.01/latest/rspei-1988-c-f-15.01.html
Secteur public	Règlement	<i>General Regulations (under the Freedom of Information and Protection of Privacy Act)</i>	P.E.I. Reg. EC564/02	http://www.canlii.org/en/pe/laws/regu/pei-reg-ec564-02/latest/pei-reg-ec564-02.html
Québec				
Secteur privé Avis : Déclaré « substantivement similaire » à la LPRPDE	Loi	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i>	L.R.Q. c. P- 39.1	http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html
Secteur public	Loi	<i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i>	L.R.Q. c. A- 2.1	http://www.canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html
Saskatchewan				
Certains secteurs privés et publics	Loi	<i>Health Information Protection Act</i>	S.S. 1999, c. H-0.021	http://www.canlii.org/en/sk/laws/stat/ss-1999-c-h-0.021/latest/ss-1999-c-h-0.021.html
Certains secteurs privés et publics	Règlement	<i>Health Information Protection Regulations (under the Health Information Protection Act)</i>	R.R.S. c. H- 0.021 Reg. 1	http://www.canlii.org/en/sk/laws/regu/rrs-c-h-0.021-reg-1/latest/rrs-c-h-0.021-reg-1.html
Yukon				
Secteur public	Loi	<i>Loi sur l'accès à l'information et à la protection de la vie privée</i>	R.S.Y. 2002, c. 1, as modifié par .Y. 2003, c. 20	http://www.gov.yk.ca/legislation/acts/atipp.pdf http://www.gov.yk.ca/legislation/acts/ataatipp.pdf
Secteur public	Règlement	<i>Règlement sur l'accès à l'information et à la protection de la vie privée (sous la Loi sur l'accès à l'information et à la protection de la vie privée)</i>	Y.D. 1996/53	http://www.canlii.org/fr/yt/legis/regl/yt-1996-53/derniere/yt-1996-53.html



Annexe B – Accord de non-divulgence à l'intention des employés/étudiants/bénévoles

Avis : Cet exemple d'accord de non-divulgence est présenté aux fins de discussions seulement. Il ne devrait être ni utilisé, ni servir de référence, sans avoir fait au préalable l'objet d'un examen de votre service juridique pour en vérifier la conformité aux lois provinciales en vigueur.

Le (la) [nom de l'organisme de santé] m'a demandé de reconfirmer mon engagement, pris lors de mon embauche, à protéger la confidentialité des informations de santé. Je reconnais que le (la) [nom de l'organisme de santé] doit rappeler périodiquement à ses employés et bénévoles leur obligation de maintenir la confidentialité; vu l'importance de cette politique, ce rappel sert à en assurer la conformité. En signant le présent document, je reconfirme que je respecterai l'engagement, énoncé ci-dessus, pris lors de mon embauche/emploi. Je confirme avoir respecté mes obligations à l'égard du maintien de la confidentialité et je m'engage à continuer à les respecter.

Le (la) [nom de l'organisme de santé] a une responsabilité légale et éthique de protéger la vie privée de tous ses patients et de conserver la confidentialité de leurs données de santé. Dans le cadre de mon embauche/emploi au [nom de l'organisme de santé], il se peut que je puisse avoir accès à des informations confidentielles sur les patients, même si je ne suis pas impliqué directement dans la prestation des services de santé.

Je comprends que de telles informations doivent être conservées en toute confidentialité. Comme condition de mon embauche/emploi au [nom de l'organisme de santé], j'accepte, par la présente, de ne divulguer, sauf à la demande de mon employeur, aucune information sur les patients à qui que ce soit ou de ne permettre à qui que ce soit d'examiner ou de faire des copies de rapports cliniques ou de tout autre document que j'aurai rédigé, reçu ou géré, ou encore, de n'utiliser les informations qu'aux fins de mon emploi.

Lorsque les dites informations doivent faire l'objet d'une discussion avec d'autres prestataires de soins de santé, je ferai preuve de discrétion et de diligence pour m'assurer que les conversations à cet égard ne puissent être entendues par des personnes non impliquées dans le dossier du patient.

Je comprends que toute violation de cette entente pourrait se traduire par des mesures disciplinaires pouvant aller jusqu'au congédiement.

Signature de l'employé/étudiant/bénévole

Date



Annexe C – Déclaration accompagnant la transmission des données de santé électroniques

Avis : Cet exemple est présenté aux fins de discussions seulement. Il ne devrait être ni utilisé, ni servir de référence, sans avoir fait au préalable l'objet d'un examen de votre service juridique pour en vérifier la conformité aux lois provinciales en vigueur.

En tant que récipiendaire de ces données contenues dans les dossiers de santé électroniques, il vous est interdit de les utiliser à des fins autres que celles pour lesquelles elles sont prévues. Vous ne pouvez les divulguer à un tiers que dans les cas suivants :

1. Si vous avez obtenu une autorisation écrite du patient ou de son représentant légal;
2. Si requis ou autorisé par les lois provinciales en vigueur.

Vous devez détruire les données dès que vous n'en aurez plus besoin.



Annexe D – Exemple d'un accord couvrant la transmission électronique des données de santé

Avis : Cet exemple d'accord est présenté aux fins de discussions seulement. Il ne devrait être ni utilisé, ni servir de référence, sans avoir fait au préalable l'objet d'un examen de votre service juridique pour en vérifier la conformité aux lois provinciales en vigueur.

Cet accord s'applique à l'ensemble des données de santé transmises électroniquement par [nom du physiothérapeute; établissement des soins de santé ou corporation] et [nom de l'autre partie, p. ex. : agence de financement] [« données de santé »], en lien avec leurs [relations d'affaires]. En contrepartie de, et moyennant les [relations d'affaires], [nom de l'autre partie] accepte de ne recueillir, de ne utiliser, de ne divulguer et de ne gérer, de quelque façon que ce soit, les données de santé, qu'en conformité aux lois sur la protection de la vie privée et aux politiques de confidentialité établies par [nom du physiothérapeute; établissement des soins de santé ou corporation] et incluant, mais ne se limitant pas, aux suivantes :

1. S'assurer que toutes les données de santé soient conservées de façon sécuritaire et empêcher l'accès non autorisé à ses équipements et systèmes informatiques utilisés pour la conservation et la transmission des données de santé électroniques, et
2. S'assurer que les données de santé soient, en tout temps, conservées dans la confidentialité la plus totale et non divulguées aux personnes/entités non autorisées à y avoir accès, ou utilisées de façon inappropriée.

En outre, [nom de l'autre partie] accepte :

1. D'utiliser les données de santé seulement aux fins de prestation de services auprès de/du [nom du physiothérapeute; établissement des soins de santé ou corporation] dans le cadre de leurs [relations d'affaires], et
2. De divulguer les dites informations seulement à ses employés ou agents qui devraient y avoir accès, afin de fournir des services à/au [nom du physiothérapeute; établissement des soins de santé ou corporation] dans le cadre de leurs [relations d'affaires], et qui ont signé une entente de confidentialité offrant substantivement la même protection de la confidentialité que celle du présent accord.

Si l'une ou l'autre des parties utilisent les services d'un tiers pour transmettre, cataloguer ou traiter les données de santé, celles-ci devront obtenir au préalable une entente auprès du tiers, qui offre substantivement la même protection de la confidentialité que celle du présent accord; en outre, l'une ou l'autre des parties sera tenue responsable de tout acte, de tout manquement ou de toute omission occasionnés par le tiers lors de la prestation de ses services. Aux fins de cette entente, le tiers sera considéré comme un agent de l'une ou de l'autre partie.

De plus, [nom de l'autre partie] accepte d'indemniser [nom du physiothérapeute; établissement des soins de santé ou corporation] et de ne pas le considérer comme imputable de tout dommage, perte, frais, engagement et dépenses résultant d'une violation du présent accord par [nom de l'autre partie], ses employés ou ses agents.

En vertu de cet accord, les obligations de [nom de l'autre partie] incluant, mais ne se limitant pas, à ses responsabilités pour le maintien de la sécurité et de la confidentialité des données de santé, continueront au-delà de la fin des [relations d'affaires]. À la fin des [relations d'affaires] ou à la demande de [nom du physiothérapeute; établissement des soins de santé ou corporation], toutes les données de santé devront être retournées sous forme appropriée à/au [nom du physiothérapeute; établissement des soins de santé ou corporation], ou encore, purgées électroniquement de façon acceptable à/au [nom du physiothérapeute; établissement des soins de santé ou corporation]; en outre, aucune copie des dites données ne peut être conservée par [nom de l'autre partie].

Signature du [nom du physiothérapeute; établissement des soins de santé ou corporation]

Date

Signature du [nom de l'autre partie]

Date

