

LE DOSSIER DE SANTÉ ÉLECTRONIQUE:

le contrôle des données personnelles de santé dans un
contexte d'informatisation des dossiers médicaux

Rapport final du projet
présenté au Commissariat à la vie privée du Canada



31 mars 2010

Rapport publié par :



6226 rue Saint-Hubert, 3^e étage
Montréal (Québec) H2S 2M2

Téléphone : 514-521-6820
Sans frais : 1 888 521-6820
Télécopieur : 514-521-0736

union@consommateur.qc.ca
www.consommateur.qc.ca/union

Membres de l'Union des consommateurs

ACEF Abitibi-Témiscamingue
ACEF Amiante – Beauce – Etchemins
ACEF de l'Est de Montréal
ACEF de l'Île-Jésus
ACEF de Lanaudière
ACEF Estrie
ACEF Grand-Portage
ACEF Montérégie-est
ACEF du Nord de Montréal
ACEF Rive-Sud de Québec
Association des consommateurs
pour la qualité dans la construction
Membres individuels

L'Union des consommateurs est membre de l'Organisation internationale des consommateurs (CI), une fédération regroupant 220 membres en provenance de 115 pays.

Rédaction du rapport

- Élisabeth Gibeau et Me Anthony Hémond

Direction de rédaction

- Me Marcel Boucher

L'Union des consommateurs remercie le Commissariat à la vie privée du Canada pour l'aide financière accordée à ce projet de recherche. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles du Commissariat à la vie privée du Canada ou du Gouvernement du Canada.

L'usage du masculin, dans ce rapport, a valeur d'épicène.

© Union des consommateurs — 2010

TABLE DES MATIÈRES

L'UNION DES CONSOMMATEURS, LA FORCE D'UN RÉSEAU	5
1. INTRODUCTION	6
2. PRÉSENTATION DU DOSSIER DE SANTÉ ÉLECTRONIQUE	8
3. LES DSE AU CANADA	10
3.1 Inforoute santé du canada, maître d'œuvre des projets	10
a) Les 10 programmes d'investissement d'Inforoute Santé du Canada	11
3.2 Projets de DES dans les provinces	13
a) DSE en Ontario	13
Modèle de gouvernance	13
Priorités adoptées	14
Avancement des projets	16
b) DSE en Colombie-Britannique	16
Modèle de gouvernance	16
Priorités adoptées	18
Avancement des projets	19
Accueil réservé aux projets de santé électronique en Colombie-Britannique	19
c) DSE au Québec	20
Modèle de gouvernance	20
Priorités adoptées	20
Avancement des projets	21
Accueil réservé aux projets de dossier de santé électronique au Québec	22
3.4 Synthèse des projets DES étudiés	23
4. CARACTÈRE FONDAMENTAL DE PROTECTION DE LA VIE PRIVÉE	24
4.1 Du cadre général de la protection des renseignements personnels à la spécificité des renseignements personnels touchant la santé	28
a) Particularité de l'information portant sur la santé	28
b) Cadre général de la protection des renseignements personnels	28
c) Compétence concurrente entre le Parlement fédéral et les législatures provinciales en matière de santé	32
d) Lois spécifiques sur la protection des renseignements personnels sur la santé en Ontario	32
e) Lois sur la protection des renseignements personnels au Québec	34
f) Lois relatives à la protection des renseignements personnels en Colombie-Britannique	35

4.2	Finalité et fondement du consentement de l'utilisateur pour la collecte, l'utilisation et la divulgation des renseignements personnels:	36
a)	Remarques sur le consentement	40
b)	Exceptions à l'exigence du consentement	41
4.3	Accès aux renseignements personnels sur la santé	47
a)	Accès par le patient à ses renseignements personnels	47
b)	Exceptions au droit d'accès	49
c)	Accès contrôlé au dossier de santé électronique	50
d)	Verrou ou masquage des informations	50
e)	Problématiques des <i>lock box</i> et autres mesures identiques	52
f)	Contrôle d'accès <i>a posteriori</i>	53
4.4	Risques d'atteinte à la vie privée relatifs aux dossiers de santé électronique	54
a)	Identifiant unique comme moyen de dépersonnalisation des renseignements personnels	56
b)	Utilisations secondaires des renseignements personnels de santé	57
4.5	Capacité des lois à répondre aux problématiques	60
5.	CONCLUSION	64

L'UNION DES CONSOMMATEURS, la force d'un réseau

L'Union des consommateurs est un organisme à but non lucratif qui regroupe plusieurs Associations coopératives d'économie familiale (ACEF), l'Association des consommateurs pour la qualité dans la construction (ACQC) ainsi que des membres individuels.

La mission de l'Union des consommateurs est de représenter et défendre les droits des consommateurs, en prenant en compte de façon particulière les intérêts des ménages à revenu modeste. Les interventions de l'Union des consommateurs s'articulent autour des valeurs chères à ses membres : la solidarité, l'équité et la justice sociale, ainsi que l'amélioration des conditions de vie des consommateurs aux plans économique, social, politique et environnemental.

La structure de l'Union des consommateurs lui permet de maintenir une vision large des enjeux de consommation tout en développant une expertise pointue dans certains secteurs d'intervention, notamment par ses travaux de recherche sur les nouvelles problématiques auxquelles les consommateurs doivent faire face; ses actions, de portée nationale, sont alimentées et légitimées par le travail terrain et l'enracinement des associations membres dans leur communauté.

L'Union des consommateurs agit principalement sur la scène nationale, en représentant les intérêts des consommateurs auprès de diverses instances politiques, réglementaires ou judiciaires et sur la place publique. Parmi ses dossiers privilégiés de recherche, d'action et de représentation, mentionnons le budget familial et l'endettement, l'énergie, les questions liées à la téléphonie, la radiodiffusion, la télédistribution et l'inforoute, la santé, l'alimentation et les biotechnologies, les produits et services financiers, les pratiques commerciales, ainsi que les politiques sociales et fiscales.

Finalement, dans le contexte de la globalisation des marchés, l'Union des consommateurs travaille en collaboration avec plusieurs groupes de consommateurs du Canada anglais et de l'étranger. Elle est membre de l'*Organisation internationale des consommateurs* (CI), organisme reconnu notamment par les Nations Unies.

1. INTRODUCTION

Les technologies de l'information et de la communication modifient en profondeur les pratiques médicales et les relations entre patients et professionnels de la santé, partout dans le monde. Qu'il s'agisse de télémédecine (télédiagnostic, télésurveillance, télé-encadrement, télé-chirurgie,...) ou de cyber-santé (gestion en ligne des dossiers médicaux, informations et prestations sur l'Internet,...), le changement des pratiques ne peut se faire sans questionnements sur la finalité des nouveaux outils, le respect de la déontologie médicale et des droits de la personne ou encore sur la transformation des pratiques professionnelles et de la confiance qui repose sur la confidentialité dans la relation entre le patient et son médecin.

Améliorer les soins aux patients, réduire le temps d'attente, rendre le système de santé plus efficient, mieux gérer les maladies chroniques, réduire les erreurs de prescription grâce aux ordonnances électroniques; tels sont certains des objectifs visés par l'informatisation du secteur de la santé. La clé de voûte de ces bénéfices attendus: une meilleure circulation de l'information dans le réseau de la santé.

Comme l'affirme Inforoute Santé du Canada :

«La prestation des soins de santé au Canada est une entreprise vaste et diffuse. Elle met en jeu une foule d'intervenants et de points de service- près de 400 000 omnipraticiens, pharmaciens locaux, infirmières et infirmiers; plus de 700 hôpitaux; et de nombreux centres de soins communautaires. Ces intervenants se rendent compte de plus en plus que la qualité des soins dans tous ces milieux exige de gérer non seulement les patients et les dépenses, mais aussi un autre aspect essentiel : la diffusion de l'information sur la santé. Et, au même titre que les autres entreprises dont l'activité dépasse les 100 milliards de dollars, le système de santé canadien doit miser sur une infrastructure informationnelle solide pour assurer la qualité des soins et optimiser sa gestion par une supervision adéquate»¹

Le Canada, à l'instar de plusieurs autres pays, semble donc se diriger vers une gestion décloisonnée des renseignements de santé, c'est-à-dire vers la centralisation des renseignements de santé et leur gestion par un seul organisme. Or, la confidentialité de ces renseignements dépend étroitement de leur mode de gestion. C'est pourquoi la question du contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux mérite l'attention de la population canadienne, jusqu'à présent fort peu consultée dans l'élaboration de ces projets.

Comme le soulignait la Commission d'accès à l'information du Québec, en 2002 :

« Le caractère sensible des données de santé n'est plus à démontrer. Pas plus d'ailleurs que la nécessité de traiter cette information dans le respect du droit au secret professionnel et du droit à la protection des renseignements personnels. Un bris de la confidentialité des renseignements de santé peut également porter atteinte au respect de

¹ INFOROUTE SANTÉ DU CANADA. DSE, *Vision 2015 : l'évolution de la nouvelle génération de soins de santé au Canada*, s.d. p. 4. [En ligne] <http://www2.infoway-inforoute.ca/Documents/InfowayVision-FR-FINAL%5B1%5D.pdf> (page consultée le 15 juillet 2009).

la réputation d'une personne, à sa vie privée ou encore favoriser la discrimination fondée sur son état de santé »²

Un sondage réalisé en 2007 pour le compte du Commissariat pour la protection de la vie privée du Canada, de Santé Canada et d'Inforoute Santé du Canada confirme que les Canadiens se préoccupent beaucoup de l'intégrité de leurs renseignements personnels, en particulier de ceux qui concernent leur santé. Ainsi, bien qu'ils approuvent à 88 % la mise au point des dossiers de santé électroniques (DSE), les préoccupations liées à la sécurité de leurs données de santé constituent le principal motif d'opposition à l'instauration de ce système. Ainsi, 45 % des personnes interrogées craignent que quelqu'un de mal intentionné s'empare de leurs renseignements; 42 % redoutent que ceux-ci servent à d'autres fins que celle d'assurer leur santé et que 37 % d'entre elles s'inquiètent de la possibilité que les personnes ayant accès à leur dossier de santé ne suivent pas la procédure établie en matière de protection et de sécurité des renseignements³.

En somme, les Canadiens sont en faveur de l'informatisation de leurs renseignements de santé, mais à condition d'être rassurés quant à leur sécurité et leur confidentialité. Comme le disait l'un des répondants au sondage, reflétant, d'après la firme Ekos, le point de vue de la majorité : « Si vous êtes capable de protéger ma vie privée, je suis à l'aise avec les [dossiers de santé électroniques] »⁴.

Qu'en est-il ? Les autorités publiques canadiennes qui travaillent actuellement à informatiser nos données personnelles de santé ont-elles pris toutes les mesures permettant d'en assurer la protection et la confidentialité alors qu'elles seront, pour la première fois, centralisées en une seule vaste banque de données ?

C'est ce que nous tenterons d'établir dans la présente recherche, en étudiant plus en profondeur les projets DSE en cours dans les provinces d'Ontario, de Colombie-Britannique et du Québec. Dans un premier temps, nous ferons une présentation des projets en cours dans ces provinces, en faisant ressortir leurs similitudes et différences. Puis, un examen des lois visant la protection des renseignements personnels, au fédéral comme au provincial, sera effectué, afin de déterminer si le cadre juridique actuel ou projeté sera suffisant, dans ce nouveau contexte d'informatisation et de centralisation des données de santé, pour offrir les garanties nécessaires.

Mais avant, débutons par une brève présentation de ce qu'est un dossier de santé électronique.

² COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Avis de la Commission d'accès à l'information concernant l'avant-projet de loi sur la carte santé au Québec*, 8 février 2002, à la page 6. [En ligne] http://www.cai.gouv.qc.ca/08_avis_de_la_cai/01_pdf/memsante.pdf (page consultée le 1^{er} septembre 2009).

³ INFOROUTE SANTÉ DU CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA ET SANTÉ CANADA. *Sondage sur les renseignements de santé électroniques et la protection de la vie privée : le point de vue des Canadiens – 2007*, août 2007, à la page 7. [En ligne] http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_FR.pdf (page consultée le 1^{er} septembre 2009).

⁴ INFOROUTE SANTÉ CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA ET SANTÉ CANADA. *Sondage sur les renseignements de santé électroniques et la protection de la vie privée : le point de vue des Canadiens – 2007*, août 2007, à la page 5. [En ligne] http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_FR.pdf (page consultée le 1^{er} septembre 2009).

2. PRÉSENTATION DU DOSSIER DE SANTÉ ÉLECTRONIQUE

La création d'un dossier de santé électronique (DSE) est la voie privilégiée par les décideurs pour assurer une meilleure circulation de l'information dans le réseau de la santé. Renfermant les données essentielles sur la santé d'une personne et relié à toutes les sources de soins au sein d'une administration publique, le DSE est une innovation qui permettra aux professionnels de la santé d'accéder à l'information essentielle sur la santé des patients, à l'endroit et au moment où ils en ont besoin, plutôt que de chercher l'information dans différents dossiers – certains sur papier, certains numériques – et dans divers systèmes.

C'est ici que se trouve la principale différence entre le DSE et le dossier médical électronique (DME). En effet, le DME est l'équivalent du dossier médical que l'on retrouve actuellement sur support papier, c'est-à-dire qu'il est le résumé d'une relation entre un patient et un professionnel de la santé et qu'il appartient à un établissement de santé ou à une clinique médicale en particulier (et demeure entre les murs de cet établissement ou clinique). Le DME contient plus d'informations que ce qui se retrouvera au DSE; on retrouve par exemple dans le DME les renseignements qui ont trait aux diagnostics et les notes des professionnels, qui ne seront pas transcrites dans le DSE.

Quant à lui, le DSE est : « un affichage intégré et sécurisé de **l'ensemble** des dossiers médicaux d'une personne, provenant de tous les systèmes du réseau; il fournit une vue globale des antécédents médicaux d'un patient. »⁵ À terme, les renseignements qu'un médecin ou autre professionnel de la santé consignera dans son DME lors de la consultation d'un patient se retrouveront automatiquement transférés dans le DSE.

De nombreux projets d'informatisation des dossiers médicaux en vue de constituer des DME sont actuellement en cours dans les cliniques médicales, hôpitaux et pharmacies du Canada. Le retard à rattraper est considérable : en effet, en 2006, 23 % des médecins canadiens utilisaient un DME, le Canada se retrouvant loin derrière les Pays-Bas, où le taux de pénétration des DME est à 98 %, la Nouvelle-Zélande (92 %), le Royaume-Uni (89 %), l'Australie (79 %) et même les États-Unis (28 %)⁶.

Nous nous concentrerons toutefois ici sur des projets qui visent la centralisation des données personnelles de santé des Canadiens en de vastes banques de données, soit les DSE.

Les enjeux sont de taille, puisque le DSE fera circuler l'information non seulement plus rapidement, mais surtout en plus grand volume et vers un plus grand nombre d'utilisateurs finaux. Le DSE vient par conséquent renverser la logique jusqu'ici applicable en la matière,

⁵ INFOROUTE SANTÉ DU CANADA. *DSE interopérable*, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-infoway/approach/investment-programs/interoperable-ehr> (page consultée le 16 juillet 2009).

⁶ THE COMMONWEALTH FUND COMMISSION ON A HIGH PERFORMANCE HEALTH SYSTEM. *Why not the best? Results from the National Scorecard on U.S. Health System Performance*, États-Unis, 2008, à la page 34 (tableau 20 Physicians Use of Electronic Medical Records). [En ligne] http://www.commonwealthfund.org/~media/Files/Publications/Fund%20Report/2008/Jul/Why%20Not%20the%20Best%20Results%20from%20the%20National%20Scorecard%20on%20U%20S%20Health%20System%20Performance%202008/Why_Not_the_Best_national_scorecard_2008%20pdf.pdf (page consultée le 21 juillet 2009).

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

passant d'un modèle de protection des renseignements basé sur la divulgation volontaire des patients à un modèle dont la principale préoccupation serait la circulation de l'information, dans lequel les entités qui fournissent les soins auront accès à l'information qui leur est nécessaire.

On retrouve deux modèles qui ont, selon les pays, servi d'architecture de base pour les DSE :
1) le dépôt de données dans des sites pivots et satellites et 2) l'échange d'information point à point.

Le premier modèle consiste à stocker les données médicales dans des dépôts gérés par une administration : c'est ce modèle qui a été adopté par le Canada, le Royaume-Uni, le *Department of Veteran Affairs* des États-Unis et Kaiser Permanente (organisation de santé américaine). Selon ce modèle, le praticien interrogera directement la base de données qui contient les renseignements sur la santé.

L'Australie, le Danemark et la Nouvelle-Zélande ont plutôt opté pour le système d'échange d'information point à point, dans lequel chaque acteur gère sa propre base de données et partage, au besoin, des éléments d'information. Ainsi, pour avoir accès à certaines données d'un patient, un professionnel de la santé devra lui en faire la demande.

	AVANTAGES	INCONVÉNIENTS
Dépôt de données dans des sites pivots	• plus facile à instaurer dans endroits où le DME n'est pas encore répandu • permet la gestion des maladies (p.ex. registre des maladies chroniques)	• résistance de la part des professionnels de la santé • mise en œuvre lente
Système d'échange d'information point à point	• mise en œuvre plus rapide • moins de résistance de la part des professionnels de la santé • coûts administratifs réduits (moins de documents papier à informatiser)	• consultation du dossier intégral du patient pas possible • gestion long terme des maladies plus difficile

Information tirée du site internet d'Inforoute Santé du Canada

3. LES DSE AU CANADA

3.1 INFOROUTE SANTÉ DU CANADA, MAÎTRE D'ŒUVRE DES PROJETS

C'est en 2000 que débute l'aventure de l'informatisation des dossiers de santé au Canada : les dirigeants politiques s'entendent alors pour mettre les technologies de l'information et des communications parmi les grandes priorités en santé, notamment par l'élaboration d'un dossier de santé électronique (DSE). Inforoute Santé du Canada (ISC), en tant que société indépendante à but non lucratif, se voit confier ce mandat la même année, et se voit octroyer un budget initial de 500 millions de dollars. En 2003, 600 millions de dollars supplémentaires sont octroyés pour la réalisation de l'objectif de base (le DSE et la télésanté), puis 100 millions supplémentaires en 2004 pour la mise au point d'un système pancanadien de surveillance de la santé publique. La mission globale d'ISC : doter la moitié de la population canadienne d'un DSE d'ici 2010.

Pour ce faire, ISC administre les fonds fédéraux en les distribuant aux provinces : cette approche pancanadienne vise à assurer l'application de normes cohérentes à l'échelle du pays (pour interopérabilité future), à proposer une même plateforme aux différentes administrations provinciales, à éviter les efforts redondants et à favoriser les économies d'échelle⁷.

Les avantages du DSE seraient nombreux : il permettrait au système de santé canadien d'économiser 6 milliards de dollars chaque année, notamment en évitant 7,5 % des erreurs de médication lors d'une hospitalisation, 15 % de tests de laboratoire non nécessaires et 32 % des attentes indues à l'urgence dues à un manque d'information sur le patient⁸. Comment ? Grâce au regroupement des renseignements dans le DSE et à leur circulation dans le réseau de la santé:

«Le DSE de base comprendra des registres des patients et des prestataires (sic), qui permettront grâce à une identification unique de consulter les images diagnostiques, les résultats de laboratoire, les profils pharmaceutiques, les rapports cliniques d'hôpitaux, les antécédents de vaccination et les rapports sur les maladies infectieuses. [...] Il s'agit d'un progrès important. Les omnipraticiens, équipés d'un ordinateur, pourront suivre les soins prodigués à leurs patients (...). Un urgentologue n'aura pas à se fier à un patient gravement malade pour connaître les médicaments qu'il prend. Le débit patients sera amélioré puisque plusieurs médecins d'un même hôpital pourront consulter simultanément les dossiers et les résultats de tests (p.ex. une image diagnostique), supprimant ainsi un important goulot d'étranglement. Et les patients éviteront les tests en double et n'auront plus à répéter sans cesse leurs antécédents médicaux»⁹

⁷ INFOROUTE SANTÉ DU CANADA. *DSE, Vision 2015 : l'évolution de la nouvelle génération de soins de santé au Canada*, s.d., p. 5. [En ligne] <http://www2.infoway-inforoute.ca/Documents/InfowayVision-FR-FINAL%5B1%5D.pdf> (page consultée le 15 juillet 2009).

⁸ *Electronic health records: potholes on the road to eHealth*, CBCNews.ca, 27 mai 2009. [En ligne] <http://www.cbc.ca/health/story/2009/05/27/f-electronic-health-records.html> (page consultée le 21 juillet 2009).

⁹ INFOROUTE SANTÉ DU CANADA. *DSE, Vision 2015 : l'évolution de la nouvelle génération de soins de santé au Canada*, s.d., p. 6. [En ligne] <http://www2.infoway-inforoute.ca/Documents/InfowayVision-FR-FINAL%5B1%5D.pdf> (page consultée le 15 juillet 2009).

a) Les 10 programmes d'investissement d'Inforoute Santé du Canada

Les provinces peuvent obtenir du financement pour la réalisation de leur projet DSE en faisant une demande dans le cadre d'un des dix programmes d'investissement d'ISC. Chacun de ces programmes d'investissement a sa propre stratégie de développement et concourt à créer « un réseau complet de solutions de DSE »¹⁰ devant, à terme, transformer la façon dont les Canadiens reçoivent les soins.

Les 10 programmes d'investissement sont les suivants¹¹ :

1. Registres : ce programme vise à financer l'élaboration de deux types de registres dans les provinces et territoires : le registre des « clients » (tel que nommé par ISC), qui dresse la liste de tous les patients, ainsi que de leurs renseignements personnels et un registre des « prestataires » (sic), qui est un répertoire des professionnels de la santé habilités. ISC affirme que ces registres contribueront à une meilleure prise de décision clinique et à une gestion efficace (permettant une sécurité accrue et une diminution des coûts administratifs).
2. Systèmes d'imagerie diagnostique : ce programme permettra la mise en place de systèmes permettant de recueillir, stocker, gérer, distribuer et consulter électroniquement les rapports et images de radiologie des patients, accroissant ainsi l'accessibilité du service pour les patients et la productivité des spécialistes.
3. Systèmes d'information sur les médicaments : ce programme finance le développement d'un système permettant l'accès, la gestion, le partage et la sauvegarde du profil pharmaceutique des patients. La possibilité de vérifier ainsi les allergies ou les interactions médicamenteuses diminuera les coûts du système de santé en réduisant le nombre d'hospitalisations ou de décès liés à des réactions suite à la prise de médicaments contre-indiqués.
4. Systèmes d'information de laboratoire : ce programme finance la création de bases de données rendant accessibles à tous les professionnels autorisés les résultats de tests de laboratoire, quel que soit le lieu, favorisant ainsi un diagnostic/traitement plus rapide et la répétition inutile de tests (réduction des coûts).
5. DSE interopérable : ce programme permettra d'assurer l'affichage intégré et sécurisé de l'ensemble des dossiers médicaux d'une personne, provenant de tous les systèmes du réseau, fournissant ainsi une vue globale des antécédents médicaux d'un patient. L'amélioration de l'accès aux services de santé, de la qualité des soins, de la sécurité et de l'efficacité du système de santé sont les bénéfices entrevus pour les Canadiens grâce au DSE.
6. Télésanté : ce programme vise à donner aux habitants des régions éloignées et rurales un meilleur accès aux soins de santé pertinents, sans déplacement et en temps opportun.
7. Surveillance de la santé publique : ce programme finance le développement de solutions pour la détection, la gestion et le contrôle des maladies infectieuses.
8. Innovation et adoption : financement de projets dont la mise en œuvre est rapide et qui favorisent l'adoption du DSE au Canada.
9. Infostructure : ce programme finance l'élaboration d'une architecture et de normes

¹⁰ INFOROUTE SANTÉ DU CANADA. *Les programmes d'investissement d'Inforoute*, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-infoway/approach/investment-programs> (page consultée le 16 juillet 2009).

¹¹ INFOROUTE SANTÉ DU CANADA. *Les programmes d'investissement d'Inforoute*, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-infoway/approach/investment-programs> (page consultée le 16 juillet 2009).

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

permettant d'assurer l'interopérabilité des DSE au Canada.

10. Accès des patients à des soins de qualité : ce programme finance les initiatives qui mettent à profit des technologies existantes d'information électronique sur la santé pour réduire les temps d'attente et améliorer l'accès aux services de santé (comprend les mesures destinées au grand public, tels que les outils de gestion des maladies chroniques, portails à l'intention des patients et ordonnancement).

En date du 31 mars 2009, selon Inforoute Santé du Canada, 173 projets en santé électronique étaient soit en phase de mise en œuvre, soit terminés et opérationnels¹². Le financement de 110 autres projets avait été approuvé, à l'échelle canadienne. Voici la répartition des 173 projets entamés ou terminés au 31 mars 2009, toutes provinces confondues :

PROGRAMME D'INVESTISSEMENT	Nombre de projets en cours	% du total
Registres	20	11,5 %
Systèmes d'imagerie diagnostique	24	14 %
Systèmes d'information- médicaments	15	9 %
Systèmes d'information de laboratoire	4	2 %
DSE interopérable	19	11 %
Télésanté	48	28 %
Surveillance de la santé publique	9	5 %
Innovation et adoption	20	11,5 %
Infostructure	9	5 %
Accès des patients à des soins de qualité	5	3 %

En somme, 28 % des projets concernent la télésanté et 52,5 %, l'une ou l'autre des composantes du DSE¹³.

¹² INFOROUTE SANTÉ DU CANADA. *Cartogramme des progrès en santé électronique*, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-progress-map> (page consultée le 16 juillet 2009).

¹³ Une remarque au bas d'un tableau dans un document d'ISC affirme qu'un DSE interopérable (DSEi) complet devrait comprendre la surveillance de la santé publique, les registres, le système d'imagerie diagnostique, le système d'info-laboratoire de même que le système d'info-médicaments. Il est précisé que les objectifs de télésanté ne sont pas considérés comme faisant partie des objectifs d'un DSE. INFOROUTE SANTÉ DU CANADA. *DSE, Vision 2015 : l'évolution de la nouvelle génération de soins de santé au Canada*, s.d., p. 9, tableau 3, remarque au bas du tableau. [En ligne] <http://www2.infoway-inforoute.ca/Documents/InfowayVision-FR-FINAL%5B1%5D.pdf> (page consultée le 16 juillet 2009).

3.2 PROJETS DE DSE DANS LES PROVINCES (ONTARIO, COLOMBIE-BRITANNIQUE, ET QUÉBEC)

Les trois provinces comptant le plus de projets de santé électronique en cours sont l'Ontario (30), le Québec (22) et la Colombie-Britannique (17). Nous examinerons plus en détail le modèle de gouvernance des projets, les priorités adoptées, le type de projets entamés et leur avancement. L'accueil réservé aux projets par la société civile sera aussi étudié, lorsque de l'information sur le sujet est disponible. Une grille d'analyse présentée à la fin de cette partie résumera le tout.

a) DSE en Ontario

Les 30 projets en Ontario concernent 9 des 10 programmes d'investissements (tous sauf le programme Infostructure). De ces 30 projets, 16 concernent la mise en place d'un DSE, soit 53 %.

MODÈLE DE GOUVERNANCE

Depuis l'automne 2008, c'est l'organisme eHealth Ontario qui gère l'instauration de ces programmes, suite à la fusion de la *Smart Systems for Health Agency* (SSHA, créée en 2002) et du *eHealth Program* du ministère de la Santé. Cette fusion a suivi la publication du rapport dévastateur de la firme Deloitte Consulting, qui faisait état en janvier 2007 de lacunes majeures dans la gestion de l'informatisation de la santé par le SSHA. Ainsi, la firme reprochait à l'agence de sérieux problèmes de gouvernance, l'absence de plan stratégique et le peu de résultats probants à son actif, et ce, après que 500 millions de dollars y aient été engloutis¹⁴. Le rapport mentionnait aussi que les professionnels de la santé semblaient peu au courant de ce qui se tramait au SSHA et que ceux qui l'étaient s'en montraient peu satisfaits. Enfin, le rapport révélait que la SSHA démontrait une méconnaissance inquiétante des législations concernant la confidentialité des données personnelles¹⁵.

Les objectifs de eHealth Ontario sont de mettre en place une stratégie provinciale unique, harmonisée et cohérente, concernant l'informatisation du secteur de la santé; d'avoir un seul point de chute pour le financement de tous les projets de santé électronique; d'éviter le dédoublement et/ou la fragmentation des efforts; d'inclure toutes les initiatives liées au développement d'un dossier de santé électronique et qui soient financées par la province dans le but de desservir la totalité de la population ontarienne¹⁶.

La nouvelle agence n'aura pas eu beaucoup de temps pour mettre en œuvre ces objectifs, paralysée qu'elle est depuis la démission, en juin 2009, de son président, le Dr Alan Hudson, suite à un scandale lié à 5 millions de dollars en contrats octroyés sans appels d'offre et à des dépenses exorbitantes de certains consultants¹⁷. M. Hudson, connu pour les défis qu'il avait

¹⁴ ZEIDENBERG, Jerry. *Ontario's Smart Systems for Health critiqued, aims for turnaround*, Canadian Healthcare Technology Magazine, mars 2007. [En ligne] <http://www.canhealth.com/mar07.html#07marstory2> (page consultée le 21 juillet 2009).

¹⁵ *Electronic health records: potholes on the road to eHealth*, CBCNews.ca, 27 mai 2009. [En ligne] <http://www.cbc.ca/health/story/2009/05/27/f-electronic-health-records.html> (page consultée le 21 juillet 2009).

¹⁶ eHEALTH ONTARIO. *What is the purpose of eHealth Ontario?*, s.d. [En ligne] <http://www.ehealthontario.on.ca/about/faqs.asp#3> (page consultée le 20 juillet 2009).

¹⁷ Kate Howlett et Lisa Priest, *eHealth Chairman resigns under a cloud*, The Globe and Mail, Toronto, 17 juin 2009. [En ligne] <http://www.theglobeandmail.com/news/politics/ehealth-chairman-resigns-under-a-cloud/article1185862/> et *Head of eHealth Ontario is fired amid contracts scandal, gets big package*, CBC News, 7 juin 2009. [En ligne] <http://www.cbc.ca/canada/story/2009/06/07/ehealth-kramer.html> et Alain Picard, *The real eHealth Ontario scandal isn't over Choco Bites*, The Globe and Mail, 11 août 2009. [En

relevés en contexte difficile, notamment la réduction des temps d'attente pour les chirurgies de la hanche et du genou, jouissait jusque là d'une excellente réputation. C'est la directrice générale, Sarah Kramer, elle aussi démissionnaire, qui avait amorcé le virage vers l'embauche massive de consultants, en supprimant dès son arrivée sept des neuf postes de direction au sein de eHealth Ontario. Or, l'attribution de plusieurs contrats sans appels d'offres et les rémunérations accordées ont soulevé la controverse, de même que le fait que les consultants aient chargé aux contribuables des frais pour de menues dépenses (café, breuvage, ...). Plusieurs des contrats ont été annulés suite au départ du docteur Hudson, laissant la nouvelle agence veuve de plusieurs de ses postes clés. Un président et directeur général par intérim a été nommé en août 2009¹⁸. Un rapport du vérificateur général de l'Ontario était attendu pour l'automne 2009, afin de connaître le fin mot sur les agissements de l'agence¹⁹.

La composition du conseil d'administration d'eHealth Ontario mérite mention : la présidente, Mme Rita Burak, préside aussi le *Toronto TELUS Community Board*, organisme fondé par la compagnie de télécommunications TELUS et qui vise à travailler avec la communauté de certaines villes canadiennes afin d'identifier certaines problématiques et de travailler à les résoudre²⁰. Cela n'est peut être pas anodin lorsqu'on sait que la compagnie TELUS est sur les rangs pour l'obtention de plusieurs contrats liés à l'informatisation du secteur de la santé au Canada²¹. Mentionnons aussi la présence d'une avocate et partenaire du cabinet Gowlings LLP, spécialisée en technologies de l'information, et d'un ancien haut dirigeant d'IBM Canada.

PRIORITÉS ADOPTÉES

En mars 2009 était adoptée la *Ontario's eHealth Strategy 2009-2012* (ci-après, la Stratégie), suite à une consultation menée auprès de plus de 400 partenaires et une revue des initiatives lancées au Canada et ailleurs. Le résultat de cette consultation a été l'identification de trois priorités cliniques très concrètes, reflétées dans la Stratégie :

- 1- La gestion du diabète : registre, base de données et dossier médical électronique compatible;
- 2- La gestion de la médication : ordonnances électroniques, système d'information sur les médicaments, profil de médication électronique;
- 3- Temps d'attente : prescriptions électroniques et couplage des ressources, système de compilation des salles d'urgence, système d'information des temps d'attente²².

ligne] <http://www.theglobeandmail.com/life/health/the-real-ehealth-ontario-scandal-isnt-over-chocobites/article1195611/> (pages consultées le 21 septembre 2009).

¹⁸ eHEALTH ONTARIO. *Robert Devitt appointed as new interim Chief Executive Officer of eHealth Ontario*, 4 août 2009. [En ligne] <http://www.ehealthontario.on.ca/News/RobertDevitt.asp> (page consultée le 21 septembre 2009).

¹⁹ Keith Leslie. *Critics fume over eHealth Ontario scandal*, Presse canadienne, 5 juin 2009. [En ligne] <http://www.theglobeandmail.com/news/politics/critics-fume-over-ehealth-ontario-scandal/article1171559/> (page consultée le 21 septembre 2009).

²⁰ TELUS. *TELUS community boards*. [En ligne] http://about.telus.com/community/social_responsibility/en/commitment/communityboards.html (page consultée le 21 septembre 2009).

²¹ Dansereau, Suzanne. *Telus : votre dossier médical sur cellulaire*, journal Les Affaires, 25 juin 2009. [En ligne] <http://www.lesaffaires.com/article/0/technologies/2009-06-25/495251/telus--votre-dossier-meteacutedical-sur-cellulaire.fr.html> (page consultée le 21 septembre 2009).

²² eHEALTH ONTARIO. *Ontario's eHealth Strategy 2009-2012*, Ontario, mars 2009, à la page 13. [En ligne] <http://www.ehealthontario.on.ca/pdfs/About/eHealthStrategy.pdf> (page consultée le 20 juillet 2009).

Nous voyons que les priorités adoptées ne mentionnent que trois des aspects du dossier de santé électronique (et rien sur le DSEi). Comme l'affirme l'organisme :

*“Investments in eHealth are underway in many jurisdictions across Canada and abroad. In many cases, they are focused on modernizing healthcare IT infrastructure and implementing Electronic Health Records (EHRs). Although Ontario aspires to similar long-term objectives, our eHealth Strategy is focused on three clinical priorities – diabetes management; medication management; wait times. In pursuing these immediate clinical imperatives, a strong infrastructure of key systems will be implemented across Ontario. As a result, many of the key cornerstones necessary for a comprehensive Ontario EHR will be in place by 2012 – which will position the province well for achieving its stated goal of a comprehensive EHR by 2015.”*²³

L'objectif de doter tous les Ontariens d'un dossier de santé électronique serait donc atteint d'ici 2015, mais en complétant d'abord l'instauration de plusieurs systèmes clés profitant directement aux patients. En effet, eHealth Ontario met beaucoup l'accent sur le fait qu'il est important que les projets de santé électronique bénéficient directement aux patients (« For excellence in healthcare, the Strategy must provide significant clinical value to patients and clinicians », p. 12). Ainsi, une étude de sept projets de santé électronique, en Ontario, en Alberta, au Danemark et au Royaume-Uni, permet de dégager des « leçons », qui ont toutes plus ou moins trait au fait que pour remplir ses objectifs et profiter du support des professionnels de la santé et des patients, les projets de santé électronique doivent impérativement leur profiter en premier lieu. Par exemple, la leçon apprise de l'étude du *UK National Care Records Service*: « Projects that are driven by a top-down emphasis on technology development without a clear clinical business case will generate resistance, delays and cost overruns »²⁴.

La réalisation de ces trois priorités ne sera possible que grâce à l'exploitation de nombreux systèmes d'information permettant l'entrée et la circulation des données cliniques, de façon efficace et sécuritaire et ce, tout au long de la chaîne de soins. C'est pourquoi eHealth Ontario a identifié quatre systèmes d'information essentiels comme étant ses « foundational priorities » pour les trois prochaines années : systèmes d'informations essentielles - « Cornerstone Information System » -, systèmes d'information sur les activités cliniques - « Clinical Activity Information Systems », services technologiques - « Technology Services » - et système de gestion des talents et des meilleures pratiques - « Enabling Practices and Talent Management ».

L'organisme prend soin de préciser que ces systèmes doivent venir en support à l'instauration des priorités cliniques d'ici 2012, bien qu'ils soient aussi essentiels à l'élaboration d'un dossier de santé électronique d'ici 2015 :

«It is critical to keep in mind that the foundational priorities are precisely that : they are the foundation that supports achieving clinical priorities in 2009-2012. In addition to

²³ eHEALTH ONTARIO. Section FAQ [En ligne] <http://www.ehealthontario.on.ca/about/faqs.asp> (page consultée le 20 juillet 2009).

²⁴ eHEALTH ONTARIO. *Ontario's eHealth Strategy 2009-2012*, Ontario, mars 2009, à la page 9. [En ligne] <http://www.ehealthontario.on.ca/pdfs/About/eHealthStrategy.pdf> (page consultée le 21 juillet 2009). Les autres leçons se trouvent aux pages 7 à 10.

supporting future clinical priorities beyond 2012, the four foundational priorities are fundamental for building a comprehensive electronic health record by 2015²⁵»

Le tableau intitulé *The Ontario eHealth Strategy 2009-2012, Priorities and Solution* résume bien l'ensemble de la stratégie élaborée par l'organisme, tout en illustrant clairement la relation entre les priorités cliniques et les « foundational priorities » de même que la place réservée au DSE²⁶.

AVANCEMENT DES PROJETS

Le cartogramme des progrès en santé électronique, disponible sur le site d'ISC, nous renseigne sur l'avancée des projets en Ontario. Ainsi, sur les 30 projets entamés par la province, 11 étaient terminés en septembre 2009 et 19 étaient toujours en cours²⁷. Les projets terminés concernent en majorité la télésanté (5). Les autres *sont répartis entre le programme « Innovation et adoption » (3) et des projets liés au DSE (3 – imagerie diagnostique et médicaments)*.

b) DSE en Colombie-Britannique

Depuis 2005, la Colombie-Britannique travaille à instaurer « un système intégré et interopérable au sein duquel l'information sur la santé est accessible, là et quand elle est nécessaire, pour aider à la santé personnelle, à la prise de décisions liées à la santé et à assurer la pérennité du système de santé » (notre traduction)²⁸. Elle a pour ce faire entamé 17 projets, répartis dans 8 des 10 programmes (tous sauf infostructure et accès des patients à des soins de qualité)²⁹. De ces 17 projets, 11 concernent la mise en place d'un DSE, soit 65 %.

MODÈLE DE GOUVERNANCE

Au départ, c'est sous la houlette du ministère de la Santé, et de son *eHealth Steering Committee*, que se développent les projets de santé électronique.³⁰ Mais, en avril 2008, la structure de gouvernance se complexifie. Ainsi, bien que ce soit toujours le ministère de la Santé qui supervise l'ensemble des projets (par son *Leadership Council*), c'est un ensemble d'organisations qui assurent leur implantation au sein du réseau de la santé : *eHealth Strategy Council* (pour la définition des priorités et la gestion du budget), *eHealth Deployment Task*

²⁵ eHEALTH ONTARIO. *Ontario's eHealth Strategy 2009-2012*, Ontario, mars 2009, à la page 12. [En ligne] <http://www.ehealthontario.on.ca/pdfs/About/eHealthStrategy.pdf> (page consultée le 21 juillet 2009).

²⁶ eHEALTH ONTARIO. *Ontario's eHealth Strategy 2009-2012*, Ontario, mars 2009, à la page 13. [En ligne] <http://www.ehealthontario.on.ca/pdfs/About/eHealthStrategy.pdf> (page consultée le 21 juillet 2009).

²⁷ INFOROUTE SANTÉ DU CANADA. Les projets en Ontario, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-progress-map?view=province&id=9%3Aontario> (page consultée le 20 septembre 2009).

²⁸ «The vision for eHealth in British Columbia can be summarized as follows: an integrated, interoperable eHealth system in which health care information is accessible, when and where it is needed, to support personal health, health care decision making and health system sustainability»

BRITISH COLUMBIA MINISTRY OF HEALTH. *eHealth Strategic Framework, British Columbia eHealth Steering Committee*, 2005, à la page 7. [En ligne] http://www.health.gov.bc.ca/library/publications/year/2005/ehealth_framework.pdf (page consultée le 27 juillet 2009).

²⁹ La liste détaillée des projets en cours se trouve à l'adresse suivante : <http://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-progress-map?view=province&id=2%3Abritish-columbia> (page consultée le 22 juillet 2009).

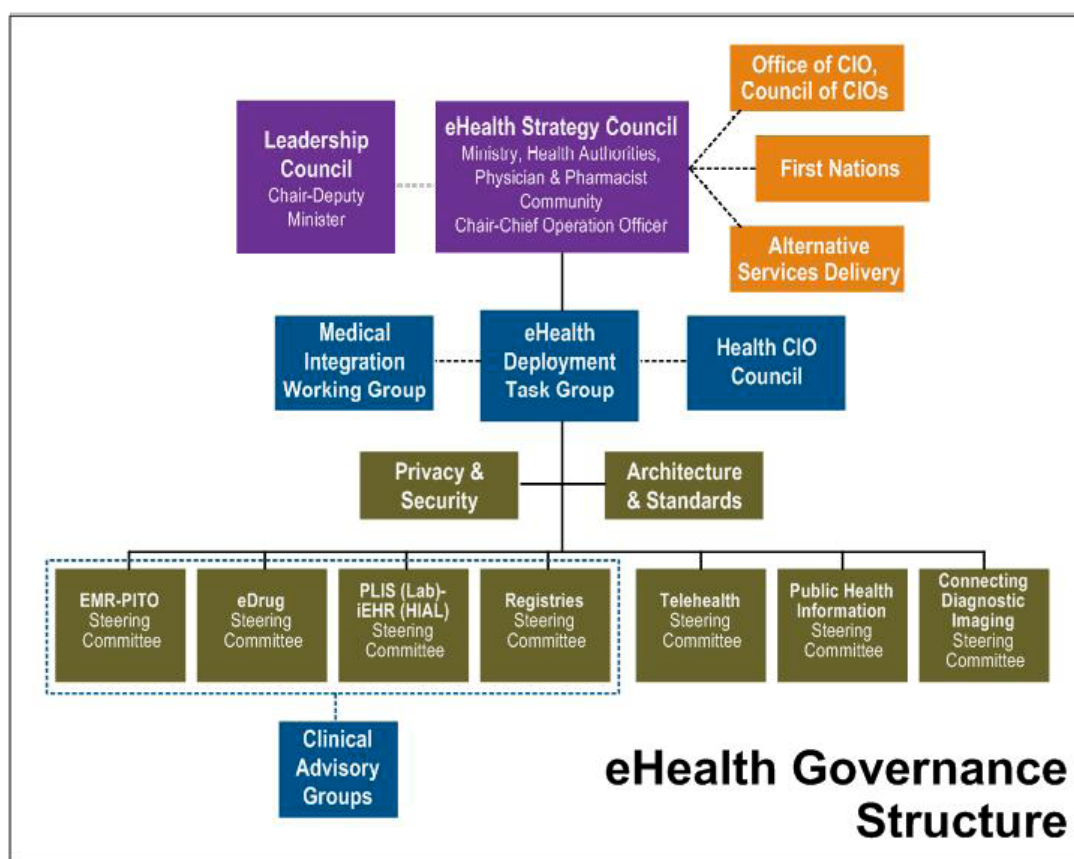
³⁰ BRITISH COLUMBIA MINISTRY OF HEALTH. *eHealth Strategic Framework, British Columbia eHealth Steering Committee*, 2005, tableau 2 de la page 11. [En ligne] http://www.health.gov.bc.ca/library/publications/year/2005/ehealth_framework.pdf (page consultée le 27 juillet 2009).

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

Group (définition et implantation des projets approuvés par le Council), *Medical Integration Working Group* (évaluation clinique des projets), *Health CIO Council* (service-conseil sur les aspects technologiques des projets) et enfin, les *Steering Committees* (responsables de l'implantation d'un projet en particulier)³¹.

En juillet 2009, d'autres changements à la structure de gouvernance sont communiqués : ainsi, au *Leadership Council* se sont ajoutés plusieurs membres, pour épauler le Ministre dans la planification stratégique. L'*eHealth Strategy Council*, le *Health CIO Council* et les *Steering Committees* conservent sensiblement le même mandat. Le *eHealth Deployment Task Group* a disparu et ses responsabilités semblent avoir été transférées au *Strategy Council*. Le *Medical Integration Working Group* est devenu le *Clinical Integration Advisory Council*, mais conserve le même mandat. Par contre, deux instances se sont ajoutées à la structure : le *Privacy & Security Group*, chargé de s'assurer de la sécurité et de la confidentialité des données de santé et l'*Architecture Group*, responsable des normes et de l'architecture des projets de santé électronique.

Le diagramme suivant donne une vue d'ensemble de cette structure de gouvernance³² :



³¹ BRITISH COLOMBIA MINISTRY OF HEALTH. *eHealth Newsletter*, avril 2008, à la page 1. [En ligne] http://www.health.gov.bc.ca/ehealth/pdf/eHealth_Newsletter_April_2008.pdf (page consultée le 27 juillet 2009).

³² BRITISH COLOMBIA MINISTRY OF HEALTH. *eHealth Newsletter*, juillet 2009, à la page 3. [En ligne] http://www.health.gov.bc.ca/ehealth/pdf/eHealth_Newsletter_July_2009.pdf (page consultée le 27 juillet 2009).

PRIORITÉS ADOPTÉES

La cybersanté doit, selon le ministère de la Santé et son Leadership Council, répondre aux cinq objectifs stratégiques suivants³³ :

- 1- Favoriser l'accès des Britanno-Colombiens aux services de santé et à l'information leur permettant d'assurer une meilleure santé;
- 2- Offrir du support aux professionnels de la santé, par la réduction des pertes de temps liées à la recherche d'information ou à la duplication de tests et par l'amélioration des relations entre les pairs;
- 3- Améliorer les capacités de planification de la santé publique par une meilleure gestion des maladies infectieuses et la disponibilité de données agrégées;
- 4- Accroître la collaboration entre professionnels de la santé par la possibilité de recevoir des images diagnostiques numérisées et l'accès aux résultats de tests laboratoires et à l'historique médical en ligne;
- 5- Assurer la pérennité de l'infrastructure technologique grâce à des registres patients efficaces et à la confidentialité garantie des données de santé.

Le plan stratégique publié en 2005 évoque une implantation sur dix ans, en trois phases, pour atteindre les objectifs visés :

Phase 1 - Accès à l'information clinique prioritaire : implanter les systèmes de base au cours des trois prochaines années afin de permettre l'accès à l'information clinique prioritaire, telle l'information concernant les médicaments ou les tests de laboratoire

Phase 2 – Renforcement des capacités et offre d'outils basés sur le savoir : faciliter les décisions cliniques et l'expansion de la Télésanté

Phase 3 – Intégration des systèmes tout au long de l'offre de services de santé : rendre possible le travail d'équipe dans des situations complexes³⁴

La phase 1 incluait la mise en place des projets précis suivants, d'ici 2008 :

- *Provider Engagement*
- *Chronic Disease Management – Integration*
- *Provincial Surgical Services Project (PSSP) - Registry*
- *InterRAI Implementation – Home Care and Residential*
- *Health Surveillance – BC Implementation of Pan-Canadian Solution*
- *Immunization Data and Physician Office Strategy*
- *Provincial Lab Information Solution*
- *Provincial eDrug Project*
- *Provincial Diagnostic Imaging – Archive and Viewer*
- *BC NurseLine Initiative*
- *Telehealth Strategic Plan*
- *Telehealth Video/Conference Scheduling System³⁵*

³³ BRITISH COLUMBIA MINISTRY OF HEALTH. *eHealth Newsletter*, avril 2008, à la page 3. [En ligne] http://www.health.gov.bc.ca/ehealth/pdf/eHealth_Newsletter_April_2008.pdf (page consultée le 28 juillet 2009).

³⁴ BRITISH COLUMBIA MINISTRY OF HEALTH. *eHealth Strategic Framework, British Columbia eHealth Steering Committee*, 2005, page 15. [En ligne] http://www.health.gov.bc.ca/library/publications/year/2005/ehealth_framework.pdf (page consultée le 28 juillet 2009).

AVANCEMENT DES PROJETS

Le cartogramme des progrès en santé électronique, disponible sur le site d'ISC, nous renseigne sur l'avancée des projets en Colombie-Britannique. Ainsi, sur les 17 projets entamés par la province, 7 étaient terminés en juillet 2009 et 10 étaient toujours en cours³⁶. Les projets terminés concernent l'imagerie diagnostique, les registres patients et prestataires et la télésanté.

ACCUEIL RÉSERVÉ AUX PROJETS DE SANTÉ ÉLECTRONIQUE EN COLOMBIE-BRITANNIQUE

En avril 2009, une coalition de plusieurs organismes a lancé l'initiative « BC Big Opt Out », en créant un site web destiné à informer la population et les professionnels de la santé des menaces à la confidentialité et à la sécurité des données personnelles de santé liées à leur centralisation au sein de larges banques de données gouvernementales.

La coalition exhorte les Britanno-colombiens à protéger leur droit à la vie privée en refusant que leurs renseignements personnels de santé soient livrés aux projets de cybersanté en cours dans la province. « *BC's Big Opt Out wants (1) The right of each individual to determine for themselves whether or not to participate in eHealth (effective informed consent)* ». ³⁷ Les buts de la campagne : assurer le droit de chaque individu de décider de participer ou non aux initiatives de cybersanté en cours, et la possibilité de déterminer leur degré de participation et la tenue d'une vaste et impartiale campagne d'information sur la cybersanté (ce que c'est, quels sont les choix des citoyens, etc.)³⁸.

Pour ce faire, elle invite la population à signer et remettre une lettre à son médecin, pharmacien ou technicien de laboratoire demandant que les renseignements personnels de santé ne soient pas transmis aux autorités responsables des DSE et qu'ils ne soient pas transférés ou consignés dans les DSE de la province, et insistant pour que la lettre de refus soit consignée au dossier du professionnel et au dossier électronique³⁹.

³⁵ BRITISH COLUMBIA MINISTRY OF HEALTH. *eHealth Strategic Framework, British Columbia eHealth Steering Committee*, 2005, page 49. [En ligne] http://www.health.gov.bc.ca/library/publications/year/2005/ehealth_framework.pdf (page consultée le 28 juillet 2009).

³⁶ INFOROUTE SANTÉ DU CANADA. Les projets en Colombie-Britannique, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-progress-map?view=province&id=2%3Abritish-columbia> (page consultée le 28 juillet 2009).

³⁷ Sur la page d'accueil du site web : « BC's Big Opt Out urges British Columbians to protect their right to privacy by refusing their personal health info be subject to eHealth ». BC BIG OPT OUT, avril 2009. [En ligne] <http://www.bcoptout.ca/index.html> (page consultée le 29 juillet 2009).

³⁸ BC PERSONS WITH AIDS SOCIETY. *eHealth : threat or menace ?*, mars 2009, page 31. [En ligne] <http://www.bcoptout.ca/LinksAndResources.html> (page consultée le 29 juillet 2009).

³⁹ « I am hereby advising you that, with the sole exception of this letter, I refuse to consent to having my confidential medical information that is held by you transferred, uploaded or disclosed to the Ministry of Health's eHealth system of electronic healthcare records.

Please ensure that my medical information recorded and/or generated by you is not disclosed to the eHealth system, and that this letter is recorded in your paper and electronic systems.

For more information about the BC Government's emerging eHealth system and what you can do about it, please visit www.bcoptout.ca. Yours truly ». [En ligne] www.bcoptout.ca/LetterTestingLabs.doc (page consultée le 29 juillet 2009).

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

Élaborée sur le modèle d'une campagne similaire menée au Royaume-Uni⁴⁰, l'initiative est le fruit de trois organismes : BC Civil Liberties Association, BC Persons with AIDS Society et le Freedom of Information and Privacy Association.

c) DSE au Québec

Le Dossier de santé du Québec (DSQ), le projet DSE de la province, est en cours depuis 2006. Les 22 projets au Québec concernent 8 des 10 programmes d'investissements (tous sauf les programmes Infostructure et Systèmes d'information de laboratoire). De ces 22 projets, 10 concernent la mise en place d'un DSE, soit 45 %.

MODÈLE DE GOUVERNANCE

C'est le Bureau du Dossier de santé du Québec qui s'occupe de la mise en place du DSQ. Depuis l'été 2009, il le fait sous la houlette de la Direction générale des technologies de l'information (DGTI) du ministère de la Santé et des Services sociaux (MSSS). Jusque là, un sous-ministre associé responsable du Dossier de santé du Québec chapeautait le dossier. Forte de son nouveau mandat, la DGTI déclare vouloir « accélérer la livraison des composantes Médicaments, Laboratoires et Imagerie diagnostique » en précisant que « désormais, chaque composante du DSQ sera traitée comme un projet autonome parmi le portefeuille de projets que représente le DSQ »⁴¹ (au lieu que les projets soient tous développés et déployés en même temps, comme il était initialement prévu).

Ces remaniements semblent faire suite au rapport du Vérificateur général du Québec de mars 2009, qui dénonçait les problèmes de gouvernance liés au DSQ : absence de stratégie d'arrimage entre le DME et le DSQ; retards importants pour tous les projets composant le DSQ; coûts totaux du DSQ encore inconnus; Conseil des ministres tenu dans l'ignorance du déroulement du projet; non disponibilité d'un plan de main-d'œuvre, particulièrement pour les postes clés et ceux nécessitant un transfert de connaissances; absence d'un portrait complet et à jour des contrats accordés; etc. « Notre intérêt pour le DSQ découle de son ampleur, des enjeux financiers qu'il comporte et de l'incidence sur la productivité du secteur de la santé des nouvelles pratiques qu'il instaure »⁴². En conséquence, le Vérificateur émet neuf nouvelles recommandations⁴³.

PRIORITÉS ADOPTÉES

Le besoin d'informatiser les données de santé est justifié, sur le site internet consacré au DSQ (en s'adressant aux professionnels de la santé), par les arguments suivants, présentés aux professionnels de la santé :

⁴⁰ Pour les détails sur l'initiative au Royaume-Uni : [En ligne] http://www.thebigoptout.com/?page_id=3 (page consultée le 29 juillet 2009).

⁴¹ DOSSIER DE SANTÉ.COM. *Le bulletin électronique d'information du Dossier de santé du Québec à l'intention du réseau de la santé et des services sociaux, Une vision plus claire de l'intégration du DSQ à la DGTI*, vol. 3 no 2, juillet 2009, page 1. [En ligne] <http://www.dossierdesante.gouv.qc.ca/download.php?f=2e46e909559d5089b458812d3501871e> (page consultée le 21 septembre 2009).

⁴² VÉRIFICATEUR GÉNÉRAL DU QUÉBEC. *Rapport du Vérificateur général du Québec à l'Assemblée nationale du Québec pour l'année 2009-2010, chapitre 6 (Vigie relative au projet Dossier de santé du Québec)*, mai 2009, aux pages 6 et 7. [En ligne] <http://www.vgq.gouv.qc.ca/fr/publications/rapport-annuel/2009-2010-T1/Rapport2009-2010-T1-Chap06.pdf> (page consultée le 28 août 2009).

⁴³ VÉRIFICATEUR GÉNÉRAL DU QUÉBEC. *Rapport du Vérificateur général du Québec à l'Assemblée nationale du Québec pour l'année 2009-2010, chapitre 6 (Vigie relative au projet Dossier de santé du Québec)*, mai 2009, aux pages 6-5 et 6-6. [En ligne] <http://www.vgq.gouv.qc.ca/fr/publications/rapport-annuel/2009-2010-T1/Rapport2009-2010-T1-Chap06.pdf> (page consultée le 28 août 2009).

« La mobilité grandissante de la population, la diversification ainsi que la spécialisation des soins et des services médicaux rendent de plus en plus nécessaire la circulation de l'information clinique. Concrètement, le DSQ reliera les établissements de santé, les pharmacies, les cliniques médicales et les cabinets privés, les groupes de médecine de famille, les laboratoires et les centres d'imagerie diagnostique.

L'information essentielle sur le patient et provenant de ces différents points de services sera centralisée et archivée dans des entrepôts de conservation sécurisés.

Le DSQ vous permettra ainsi de travailler de façon complémentaire en échangeant rapidement et en temps réel, l'information essentielle et structurée sur votre patient, quel que soit l'endroit du Québec où ce dernier aura reçu des soins ou des services»⁴⁴

Au gré des développements du système, les professionnels de la santé auront, selon leur profil, accès à l'ensemble ou à une partie des données suivantes :

- la liste des médicaments administrés;
- les données immunologiques (vaccins reçus au Québec);
- les rapports d'imagerie diagnostique (radiologie, résonance magnétique, échographie)
- les résultats des examens de laboratoire d'exploration fonctionnelle (électroencéphalogramme, électromyogramme, spirométrie, etc.);
- les allergies et intolérances;
- d'autres données dont le professionnel conviendrait avec le patient (coordonnées des professionnels de la santé consultés et information essentielle à connaître en cas d'urgence: traitements, port d'orthèses ou d'un stimulateur cardiaque, etc.)⁴⁵.

Toutes les données, sauf celles de la dernière catégorie, seront obligatoirement consignées dans le DSQ et mises à jour automatiquement, à chaque visite du patient à l'un des professionnels de la santé habilités.

La DGTI, responsable du dossier au ministère de la Santé depuis l'été 2009, semble accorder la priorité à l'achèvement des projets Médicaments, Laboratoire et Imagerie diagnostique⁴⁶. Or, rien ne ressemblant à un plan stratégique n'avait, en juillet 2009, été rédigé et rendu public.

AVANCEMENT DES PROJETS

Le cartogramme des progrès en santé électronique d'Inforoute Santé du Canada nous renseigne sur l'avancée des projets au Québec en août 2009. Ainsi, la totalité des 22 projets entamés par la province étaient toujours en cours d'exécution. Dix d'entre eux concernent la

⁴⁴ SANTÉ ET SERVICES SOCIAUX QUÉBEC. *Le profil de votre patient en quelques clics*, s.d. [En ligne] http://www.dossierdesante.gouv.qc.ca/fr_profil_patient.phtml (page consultée le 30 juillet 2009).

⁴⁵ SANTÉ ET SERVICES SOCIAUX QUÉBEC. *Le contenu d'un dossier santé du Québec*, s.d. [En ligne] http://www.dossierdesante.gouv.qc.ca/fr_le_contenu_du_DSQ.phtml (page consultée le 30 juillet 2009).

⁴⁶ DOSSIER DE SANTÉ.COM. *Le bulletin électronique d'information du Dossier de santé du Québec à l'intention du réseau de la santé et des services sociaux, Une vision plus claire de l'intégration du DSQ à la DGTI*, vol. 3 no 2, juillet 2009, page 1. [En ligne] <http://www.dossierdesante.gouv.qc.ca/download.php?f=2e46e909559d5089b458812d3501871e> (page consultée le 21 septembre 2009).

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

télésanté et dix autres, les projets liés à la mise en place d'un DSE⁴⁷ (imagerie diagnostique, registres, information-médicaments, surveillance de la santé publique).

ACCUEIL RÉSERVÉ AUX PROJETS DE DOSSIER DE SANTÉ ÉLECTRONIQUE AU QUÉBEC

Lorsque le Vérificateur général dresse la liste des acteurs importants liés au projet du DSQ, il prend bien soin d'identifier le citoyen, « dont le consentement libre et éclairé est essentiel à la réussite du projet »⁴⁸.

C'est bien l'avis de plusieurs membres des milieux syndicaux et communautaires québécois. C'est ainsi que, à l'initiative de la Coalition solidarité santé⁴⁹, plus de 58 organisations communautaires et syndicales ont envoyé, en avril 2009, une lettre au Ministre de la Santé demandant qu'une consultation publique ait lieu sans délai afin de permettre l'évaluation de la phase 1 du projet pilote, mais aussi celle de l'ensemble du projet:

*« Dans un premier temps, cet exercice pourrait permettre de faire l'évaluation du projet pilote de la phase I dans la région de la Capitale-Nationale. Dans un deuxième temps, il donnerait une occasion à la population, aux différentes organisations sociales, aux décideurs, aux professionnels du réseau de la santé et au ministère de la Santé de débattre les multiples questions que soulève le concept du DSQ. En outre, cette consultation pourrait éclaircir d'autres questions, cette fois relatives à la gestion des fonds publics. »*⁵⁰

De très nombreux groupes ont aussi manifesté leur opposition au projet de loi 70, adopté en mai 2008, qui venait enlever au patient la possibilité d'un consentement exprès au DSQ, en adoptant le principe du consentement présumé, selon lequel le patient doit faire la demande expresse s'il refuse d'avoir son DSQ.

⁴⁷ INFOROUTE SANTÉ DU CANADA. *Investissements d'Inforoute au Québec*, s.d. [En ligne] <http://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-progress-map> (page consultée le 28 août 2009).

⁴⁸ VÉRIFICATEUR GÉNÉRAL DU QUÉBEC. *Rapport du Vérificateur général du Québec à l'Assemblée nationale du Québec pour l'année 2009-2010, chapitre 6 (Vigie relative au projet Dossier de santé du Québec)*, mai 2009, à la page 6-11. [En ligne] <http://www.vgq.gouv.qc.ca/fr/publications/rapport-annuel/2009-2010-T1/Rapport2009-2010-T1-Chap06.pdf> (page consultée le 28 août 2009).

⁴⁹ La Coalition solidarité santé regroupe, depuis 1991, des organisations syndicales, communautaires et religieuses ainsi que des comités de citoyens, tous réunis pour que soient respectés les grands principes qui ont conduit à la mise sur pied de notre système de santé: le caractère public, la gratuité, l'accessibilité, l'universalité et l'intégralité.

⁵⁰ COALITION SOLIDARITÉ SANTÉ. *Le Dossier de santé du Québec : une consultation publique s'impose !*, 8 mai 2009. [En ligne] <http://www.newswire.ca/fr/releases/archive/May2009/08/c9719.html> (page consultée le 31 août 2009).

3.4 SYNTHÈSE DES PROJETS DSE ÉTUDIÉS

Province	Ontario	Colombie-Britannique	Québec
Investissements engagés	600 millions \$ de 2002 à 2008 2,133 milliards \$ 2009-2012	?	563 millions \$ (2006-2010)
Priorités	Depuis 2008 : - gestion du diabète - gestion de la médication - réduction des temps d'attente	Accès aux informations cliniques prioritaires (médicaments, tests laboratoire, etc.)	Depuis été 2009 : mise en place des systèmes info-médicaments, info-laboratoire et imagerie diagnostique
Échéancier	2015	2015	2011
Autorité responsable	eHealth Ontario, depuis automne 2008	eHealth Leadership Council, depuis 2009	Direction générale des technologies de l'information, du MSSS, depuis juillet 2009
Proportion des projets DSE	16 projets liés au DSE, sur 30 (53 %)	11 projets liés au DSE, sur 17 (65 %)	10 projets liés au DSE, sur 22 (45 %)
Avancée des projets (août 2009)	11 projets terminés et 19 en cours	7 projets terminés et 10 en cours	22 projets en cours (aucun de terminé)

Il est à noter que les projets DSE des trois provinces étudiées ont tous en commun d'avoir fait l'objet de nombreuses réorganisations structurelles depuis le début de leur mise en œuvre. En effet, l'ampleur des projets d'informatisation des dossiers médicaux semble causer des maux de tête aux autorités provinciales, qui peinent à tenir les ficelles de toutes les composantes des projets et à en assurer la bonne gouvernance.

La prochaine section abordera la question de l'encadrement législatif de la protection des renseignements personnels. Nous y étudierons les lois fédérales ainsi que les lois de trois provinces (Ontario, Colombie-Britannique et Québec) qui portent notamment sur les règles relatives à la collecte, à l'utilisation, à la divulgation et la gestion des renseignements, afin de déterminer si, dans un contexte d'informatisation des dossiers médicaux, les renseignements personnels de santé seront bien protégés.

4. CARACTÈRE FONDAMENTAL DE PROTECTION DE LA VIE PRIVÉE

Au niveau international, il faut constater l'importance accordée au droit à la vie privée qui a été affirmé dans de nombreux textes, notamment à l'article 17, paragraphe 1 du Pacte international relatif aux droits civils et politiques : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. »⁵¹, et à l'article 12 de la Déclaration universelle des droits de l'Homme: «Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.»⁵²

Si le Canada a ratifié ces différents textes internationaux, la Charte canadienne des droits et libertés, n'énonce toutefois pas explicitement de droit au respect de la vie privée, contrairement à la Charte des droits et libertés de la personne du Québec (L.R.Q. c. C-12). Il serait alors possible de croire que la protection de la vie privée des personnes n'est pas garantie constitutionnellement.

Cela serait se méprendre; la Cour suprême du Canada est venue préciser dans plusieurs décisions, dont *Hunter c. Southam* :

*« À l'instar de la Cour suprême des États-Unis, j'hésiterais à exclure la possibilité que le droit à la protection contre les fouilles, les perquisitions et les saisies abusives protège d'autres droits que le droit à la vie privée, mais pour les fins du présent pourvoi, je suis convaincu que la protection qu'il offre est au moins aussi étendue. La garantie de protection contre les fouilles, les perquisitions et les saisies abusives ne vise qu'une attente raisonnable. Cette limitation du droit garanti par l'art. 8, qu'elle soit exprimée sous la forme négative, c'est-à-dire comme une protection contre les fouilles, les perquisitions et les saisies «abusives», ou sous la forme positive comme le droit de s'attendre «raisonnablement» à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. »*⁵³

Peu de temps après, la Cour suprême poursuit son élaboration du concept de droit constitutionnel à la protection de la vie privée en mentionnant, dans l'arrêt *R. c. Beare*:

« À supposer que l'art. 7 assure la protection d'un droit à la vie privée comme le droit qui est inhérent à la garantie contre les fouilles, les perquisitions et les saisies abusives de l'art. 8 de la Charte, une proposition que je serais enclin à admettre, il faut se rappeler que le Juge en chef actuel, dans l'arrêt Southam, a pris soin de souligner que la

⁵¹ Pacte international relatif aux droits civils et politiques [En ligne]

<http://www2.ohchr.org/french/law/ccpr.htm> (page consultée le 9 septembre 2009), le Pacte a été ratifié par le Canada le 19 mai 1976 [En ligne]

http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (page consultée le 9 septembre 2009)

⁵² DÉCLARATION UNIVERSELLE DES DROITS DE L'HOMME [En ligne]

<http://www.un.org/fr/documents/udhr/#a12> (page consultée le 9 septembre 2009)

⁵³ HUNTER ET AL. c. SOUTHAM INC., [1984] 2 R.C.S. 145, 159

Constitution garantissait une "attente raisonnable" en ce qui concerne la protection de la vie privée (à la p. 159). »⁵⁴

Ainsi, le droit à la protection de la vie privée serait reconnu constitutionnellement par l'effet combiné des articles 7 et 8 de la Charte canadienne des droits et libertés qui disposent respectivement : « Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale. » et « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. »

La France n'a pas non plus dans sa Constitution d'article qui reconnaisse de façon explicite le droit à la protection de la vie privée. Cependant, il faut, avant de tirer des conclusions, tenir compte de l'ensemble des textes européens, et notamment de la Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales,⁵⁵ dont l'article 8 se lit comme suit: « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. » Comme au Canada, le Conseil Constitutionnel, gardien de la constitutionnalité des lois, a, dans une décision rendue en 2004, rattaché le droit à la vie privée à l'un des textes de la Constitution, à savoir la Déclaration des droits de l'Homme et du Citoyen: « Considérant, en premier lieu, qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression » ; que la liberté proclamée par cet article implique le respect de la vie privée. »⁵⁶

Ainsi, comme la Cour suprême l'a fait en interprétant certains articles de la Charte canadienne des droits et libertés comme portant sur le droit à la protection de la vie privée, le Conseil Constitutionnel a rattaché la protection de la vie privée à des articles de la Constitution française.

Similairement à ce que nous avons pu constater avec le Canada et la France, la protection de la vie privée ne figure pas non plus de façon explicite dans la Constitution des États-Unis.⁵⁷ Toutefois, et comme dans les pays cités précédemment, la plus haute juridiction, soit la Cour suprême des États-Unis, a rattaché la protection de la vie privée à certains articles de la Constitution, notamment le 4^e amendement. La décision *Olmstead*⁵⁸ est éloquent sur le sujet, et ce, même si la déclaration pertinente se retrouve dans la dissidence du juge Brandeis⁵⁹:

« The protection guaranteed by the amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness.

⁵⁴ R. C. BEARE., [1988] 2 R.C.S 387, §67

⁵⁵ CONVENTION DE SAUVEGARDE DES DROITS DE L'HOMME ET DES LIBERTÉS FONDAMENTALES [En ligne] <http://conventions.coe.int/treaty/fr/treaties/html/005.htm#FN1> (page consultée le 9 septembre 2009)

⁵⁶ DÉCISION DU CONSEIL CONSTITUTIONNEL N°2004-499 DC DU 29 JUILLET 2004 [En ligne] <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-499-dc/decision-n-2004-499-dc-du-29-juillet-2004.904.html> (page consultée le 9 septembre 2009)

⁵⁷ POSNER, Richard. The Uncertain protection of privacy by the Supreme Court, 1979 Supreme Court Review 173, 1979 «The Constitution of the United States contains no reference to privacy.»

⁵⁸ OLMSTEAD v. U.S., 277 U.S. 438(1928), la Cour était divisée sur la question (5/4)

⁵⁹ Le Juge Brandeis fut l'un des auteurs du célèbre article de la revue *Harvard law Review* qui le premier mentionna le « right to privacy ». Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)

They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.»⁶⁰

Le rattachement à la Constitution américaine de la protection de la vie privée continua progressivement et, en 1965, la décision *Griswold* arrima la protection de la vie privée à plusieurs amendements de la Constitution, dont le 4^e amendement: « We recently referred [381 U.S. 479, 485] in *Mapp v. Ohio*, 367 U.S. 643, 656, to the Fourth Amendment as creating a "right to privacy, no less important than any other right carefully and particularly reserved to the people". »⁶¹

La décision *Warden* vint préciser le fondement juridique sur lequel repose ce que l'on désigne par le terme «privacy»: «We have recognized that the principal object of the Fourth Amendment is the protection of privacy, rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.»⁶²

Finalement, dans l'affaire *Katz*, la Cour suprême a mentionné clairement : « What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.»⁶³

La vie privée est donc protégée constitutionnellement. Reste à définir ce que recouvre ce concept de « vie privée ». La définition de la vie privée est extrêmement complexe, voire presque impossible; certains auteurs s'y sont toutefois essayés. Pour certains, il s'agit du : « droit de chacun à une sphère d'intimité ou, plus précisément, le pouvoir de préserver cet espace privé de toutes immixtions.»⁶⁴ Pour d'autres: « The harsh reality is: legal privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition, yet heavily interrelated as a matter of history, such that efforts to completely sever one from another are (and have been) disastrous.»⁶⁵

Selon Geneviève Tremblay, le « droit à la vie privée est la prémisse de la protection effective des renseignements personnels. Celui-ci se définit comme le droit de chacun à une sphère d'intimité. Il comporte deux dimensions: la *protection de l'autonomie de la personne*, soit la protection des lieux découlant, notamment des garanties relatives aux perquisitions, fouilles et saisies abusives, ainsi que la protection de l'intégrité et la dignité de la personne; et la *protection de l'information*, c'est-à-dire la protection des données à caractère personnel, des

⁶⁰ OLMSTEAD v. U.S., 277 U.S. 438(1928)

⁶¹ GRISWOLD v. CONNECTICUT., 381 U.S. 479 (1965)

⁶² WARDEN v. HAYDEN., 387 U.S. 294

⁶³ KATZ v. UNITED STATES, 389 U.S. 347 (1967) 351

⁶⁴ TREMBLAY Geneviève, « L'influence du droit constitutionnel à la vie privée dans le domaine de la télémédecine », 29 Queen's L. J. (2003) 326

⁶⁵ GORMLEY Ken, « One Hundred years of privacy » 1992 Wisconsin Law Review. 1335, 1339

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

substances corporelles, des conversations téléphoniques ou électroniques et de la correspondance, ainsi que la protection contre la surveillance.»⁶⁶

Concernant la protection de l'information, la Cour suprême du Canada s'est penchée sur le droit à la vie privée en matière d'information :

« Enfin il y a le droit à la vie privée en matière d'information. Cet aspect aussi est fondé sur la notion de dignité et d'intégrité de la personne. Comme l'affirme le groupe d'étude (à la p. 13): "Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend." Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués. Tous les paliers de gouvernement ont, ces dernières années, reconnu cela et ont conçu des règles et des règlements en vue de restreindre l'utilisation des données qu'ils recueillent à celle pour laquelle ils le font; voir, par exemple, la Loi sur la protection des renseignements personnels.»⁶⁷

Un lien fort a été établi entre le droit à la vie privée et la protection des renseignements personnels, lien qui pourrait engendrer une protection constitutionnelle relativement à la divulgation des renseignements personnels et à l'usage ultérieur de ces renseignements.⁶⁸

Après ces brèves considérations sur la reconnaissance constitutionnelle de la protection de la vie privée, nous nous intéresserons aux lois spécifiques concernant les renseignements personnels.

⁶⁶ TREMBLAY Geneviève, « L'influence du droit constitutionnel à la vie privée dans le domaine de la télémédecine », 29 Queen's L. J. (2003) 335

⁶⁷ R. c. DYMENT [1988] 2 R.C.S. 417

⁶⁸ TREMBLAY Geneviève, « L'influence du droit constitutionnel à la vie privée dans le domaine de la télémédecine », 29 Queen's L. J. (2003) 339

4.1 DU CADRE GÉNÉRAL DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS À LA SPÉCIFICITÉ DES RENSEIGNEMENTS PERSONNELS TOUCHANT LA SANTÉ

a) Particularité de l'information portant sur la santé

Avant de nous intéresser au cadre général de la protection des renseignements personnels, il nous faut préciser en quoi les renseignements personnels touchant à la santé présentent des enjeux spécifiques. Cette spécificité s'explique par le fait que ces renseignements personnels, en touchant à la santé, se rattachent à l'intimité et à la dignité de la personne.⁶⁹ Il faut également en effet tenir compte des raisons qui amènent le patient à divulguer de l'information sur sa santé, à savoir l'obtention de soins de santé. Bien souvent les individus sont dans une situation de vulnérabilité et de dépendance par rapport au médecin. La Cour suprême mentionne cet état de vulnérabilité du patient dans la décision *Dyment*⁷⁰. Le patient qui souhaite obtenir des soins de santé en vue de protéger sa vie ou sa santé devra nécessairement divulguer de l'information personnelle à caractère intime, qui permettra au médecin d'établir un diagnostic et d'offrir des soins. Ces renseignements sont extrêmement sensibles parce qu'ils pourraient dans une certaine mesure être utilisés par des tiers pour ostraciser les personnes, les empêcher d'accéder à certains services (d'assurance, par exemple) ou même à des emplois. Ce sont ces particularités de l'information sur la santé qui expliquent le besoin de lois spécifiques pour la protection de ce type d'information, qui doivent compléter les lois à portée générale sur la protection des renseignements personnels.

Avant de nous intéresser aux législations ou aux dispositions particulières qui ont pu être adoptées par certaines provinces, nous nous concentrerons sur le cadre général de la protection des renseignements personnels, qui coexiste avec les régimes spécifiques mis en place dans certaines provinces.

b) Cadre général de la protection des renseignements personnels

Au Canada, s'il existe des lois fédérales et des lois provinciales sur la protection des renseignements personnels, nous devons également distinguer les lois sur la protection des renseignements personnels qui s'appliquent au secteur public de celles qui s'appliquent au secteur privé. Nous procéderons à notre synthèse de ces lois en débutant par les lois fédérales visant le secteur privé, et poursuivrons avec celles qui visent le secteur public.

Le gouvernement fédéral s'est appuyé sur la compétence que lui confèrent les dispositions relatives au commerce qui se trouvent à l'article 91(2) de la Loi Constitutionnelle de 1867 pour mettre en œuvre la Loi sur la protection des renseignements personnels et les documents électroniques (2000, ch.5) (ci-après LPRPDE).

D'ailleurs la LPRPDE vise, comme l'indique son préambule, à : « faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou

⁶⁹ TREMBLAY Geneviève, « L'influence du droit constitutionnel à la vie privée dans le domaine de la télémédecine », 29 Queen's L. J. (2003) 326, 343

⁷⁰ R. c. DYMENT [1988] 2 R.C.S. 417 « Cela est évidemment nécessaire si l'on considère la vulnérabilité de l'individu dans de telles circonstances. Il est forcé de divulguer les renseignements les plus intimes et d'autoriser les atteintes à son intégrité physique s'il veut protéger sa vie ou sa santé. Les tendances récentes en matière de santé ont exacerbé les problèmes relatifs au droit à la vie privée »

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions.»⁷¹

L'article 4 de la LPRPDE, qui se trouve à la partie 1 de la Loi (protection des renseignements personnels dans le secteur privé)⁷², se lit comme suit : « La présente partie s'applique à toute organisation à l'égard des renseignements personnels : a) soit qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales; b) soit qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre d'une entreprise fédérale.»⁷³

La partie 1 de la LPRPDE s'applique donc principalement aux « organisations » qui exercent des activités commerciales. L'article 2 définit ces deux notions :

« activité commerciale »: Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds. (...)

« organisation »: S'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales.»⁷⁴

Quoique la Loi fédérale s'applique, en principe, sur tout le territoire canadien, il faut savoir que les législatures provinciales peuvent élaborer leurs propres lois relatives à la protection des renseignements personnels, et que la LPRPDE ne s'appliquera pas aux provinces qui auront édicté des lois essentiellement similaires à la LPRPDE pour ce qui est des renseignements personnels collectés, utilisés ou communiqués à l'intérieur de la province.⁷⁵ Actuellement, l'Alberta⁷⁶, la Colombie Britannique⁷⁷ et le Québec⁷⁸ sont les seules provinces où des lois

⁷¹ Loi sur la protection des renseignements personnels et les documents électroniques, (2000, ch. 5)

⁷² La partie 2 de la LPRPDE bien qu'elle traite spécifiquement de documents électroniques, de certification, de signatures et preuves électroniques. L'article 31 définit comme suit les documents électroniques visés : « Ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés tout affichage et toute sortie imprimée ou autre de ces données » et les données : « Toute forme de représentation d'informations ou de notions ». En vertu de l'article 32 de la LPRPDE, cette partie a pour objet : « de prévoir l'utilisation de moyens électroniques, de la manière prévue dans la présente partie, dans les cas où les textes législatifs envisagent l'utilisation d'un support papier pour enregistrer ou communiquer de l'information ou des transactions. ». La partie 2 ne traite toutefois pas des règles de collecte, de conservation et de communication des renseignements personnels, les dispositions pertinentes à cet effet se trouvant toutes à la partie 1 de la Loi.

⁷³ DRAPEAU Michel, et Marc-Aurèle Racicot, Protection of privacy in the canadian private and health sectors, 2007 Thomson Canada, FED-4

⁷⁴ DRAPEAU Michel, et Marc-Aurèle Racicot, Protection of privacy in the canadian private and health sectors, 2007 Thomson Canada, FED-4

⁷⁵ L'article 26(2)b) de la LPRPDE mentionne que le gouverneur en Conseil peut par décret : « s'il est convaincu qu'une loi provinciale essentiellement similaire à la présente partie s'applique à une organisation — ou catégorie d'organisations — ou à une activité — ou catégorie d'activités —, exclure l'organisation, l'activité ou la catégorie de l'application de la présente partie à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur de la province en cause. »

⁷⁶ PERSONAL INFORMATION PROTECTION ACT, S.A. 2003, c. P-6.5

⁷⁷ PERSONAL INFORMATION PROTECTION ACT, S.B.C. 2003, c. 63

⁷⁸ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ, L.R.Q. c. P-39.1

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

adoptées par des législatures provinciales ont été reconnues essentiellement similaires à la LPRPDE⁷⁹.

La définition de renseignement personnel que l'on retrouve à la LPRPDE se lit comme suit :
« Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéro de téléphone de son lieu de travail. »

À cette définition générale, la Loi ajoute une définition propre aux renseignements personnels sur la santé, confirmant la spécificité de ce type de renseignements personnels :

« « renseignements personnels sur la santé » En ce qui concerne un individu vivant ou décédé :

- a) tout renseignement ayant trait à sa santé physique ou mentale;*
- b) tout renseignement relatif aux services de santé fournis à celui-ci;*
- c) tout renseignement relatif aux dons de parties du corps ou de substances corporelles faits par lui, ou tout renseignement provenant des résultats de tests ou d'examen effectués sur une partie du corps ou une substance corporelle de celui-ci;*
- d) tout renseignement recueilli dans le cadre de la prestation de services de santé à celui-ci; e) tout renseignement recueilli fortuitement lors de la prestation de services de santé à celui-ci.⁸⁰ »*

On doit souligner l'article 30 (1.1) de la section 5 de la LPRPDE qui précise : « (1.1) La présente partie ne s'applique pas à une organisation à l'égard des renseignements personnels sur la santé qu'elle recueille, utilise ou communique. » Une exclusion générale relative aux renseignements personnels sur la santé est ainsi édictée, il faut donc nous orienter vers d'autres lois pour connaître le régime de protection des renseignements personnels sur la santé.

Une autre loi fédérale, la Loi sur la protection des renseignements personnels (LPRP), a pour objet de « compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent. »⁸¹ Cette loi s'attache donc principalement à encadrer la protection des renseignements personnels relevant des institutions fédérales définies à l'article 3 : « « institution fédérale » a) Tout ministère ou département d'État relevant du gouvernement du Canada, ou tout organisme, figurant à l'annexe; b) toute société d'État mère ou filiale à cent pour cent d'une telle société, au sens de l'article 83 de la *Loi sur la gestion des finances publiques*. » À l'Annexe de la Loi sur la protection des renseignements personnels, nous trouvons une longue liste de ministères, et organismes gouvernementaux auxquels s'applique cette Loi sur la protection des renseignements personnels.

La Loi sur la protection des renseignements personnels donne également à l'article 3 une définition de renseignements personnels :

⁷⁹ DRAPEAU Michel, et Marc-Aurèle Racicot, *Protection of privacy in the canadian private and health sectors*, 2007 Thomson Canada, FED-4

⁸⁰ *Ibid.*

⁸¹ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, L.R.C » 1985, c. P-21, article 3

*« « renseignements personnels »: Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment : a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille; b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé; c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre; d) son adresse, ses empreintes digitales ou son groupe sanguin; e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement; f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur; g) les idées ou opinions d'autrui sur lui; h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions; i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet; (...)»⁸²
(nos soulignés).*

On constate donc que les lois fédérales identifient les renseignements personnels de santé, soit en créant une catégorie spécifique de renseignements personnels (LPRPDE), soit en nommant la santé parmi les éléments d'une énumération des objets sur lesquels peuvent porter les renseignements protégés (LPRP).

Cependant, bien que la LPRPDE définisse un cadre général pour la protection des renseignements personnels, la question de son applicabilité aux renseignements personnels de santé a soulevé des questionnements, dont celui de la Commissaire à l'information et à la vie privée de l'Ontario, qui a soulevé le caractère particulier de la protection des renseignements personnels sur la santé et mentionné que : « The requirements under PIPEDA were designed to regulate direct marketing, electronic commerce and other analogous activities and do not specifically address the unique circumstances encountered within the health care system. »⁸³

Il importe de souligner l'importance de la LPRPDE : malgré sa non applicabilité apparente aux provinces qui adoptent des lois similaires, cette loi fédérale s'appliquera malgré tout lorsqu'il y a échange de renseignements personnels interprovincial, ou avec les territoires, de même que lorsque les renseignements personnels sont transmis à d'autres pays.

Cependant, comme notre recherche s'attarde à l'étude de la protection des renseignements personnels touchant la santé, il est donc important de s'attarder à déterminer les limites des compétences concurrentes du fédéral et des provinces en matière de santé.

⁸² LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, L.R.C » 1985, c. P-21, article 2

⁸³ Frequently Asked Questions: Personal Health Information Protection Act, février 2005, p. 5. [En ligne] http://www.ipc.on.ca/images/Resources/hfaq-e_147614683716.pdf (page consultée le 12 septembre 2009)

c) Compétence concurrente entre le Parlement fédéral et les législatures provinciales en matière de santé

La Loi constitutionnelle de 1867 ne mentionne pas la santé parmi les compétences qui sont attribuées de façon exclusive au fédéral ou aux provinces. La Cour suprême a été appelée à trancher la question dans la décision *RJR-Macdonald inc. c. Canada (Procureur général)*⁸⁴, et a conclu que le Parlement et les législatures provinciales peuvent tous deux valablement légiférer dans ce domaine.⁸⁵ Aussi bien le fédéral que les législatures provinciales peuvent donc adopter des lois relatives à la protection des renseignements personnels touchant la santé, attendu que les deux paliers de gouvernement ont compétence dans ces domaines.

Les provinces de l'Alberta⁸⁶, du Manitoba⁸⁷, de l'Ontario⁸⁸ et de la Saskatchewan⁸⁹, ainsi que la Colombie-Britannique⁹⁰ ont toutes adopté des lois spécifiques relatives à la collecte, l'utilisation, et la divulgation des renseignements personnels sur la santé. Notre étude se limitera aux provinces de l'Ontario, du Québec et de la Colombie-Britannique, qui ont aussi, comme nous l'avons mentionné plus tôt, adopté leurs propres lois sur la protection des renseignements personnels.

d) Lois spécifiques sur la protection des renseignements personnels sur la santé en Ontario

La Loi de 2004 sur la protection des renseignements personnels sur la santé (L.O. 2004, c. 3) (ci-après LPRPS) a pour objet d': « établir des règles de collecte, d'utilisation et de divulgation de renseignements personnels sur la santé concernant un particulier qui protègent leur confidentialité et la vie privée du particulier à leur égard tout en facilitant la fourniture efficace des soins de santé; b) conférer au particulier le droit d'accès aux renseignements personnels sur la santé qui le concernent, sous réserve d'exceptions restreintes particulières énoncées dans la présente loi; c) conférer au particulier le droit d'exiger la rectification ou la modification de renseignements personnels sur la santé qui le concernent, sous réserve d'exceptions restreintes particulières énoncées dans la présente loi; d) prévoir l'examen indépendant et le règlement des plaintes présentées à l'égard de renseignements personnels sur la santé; e) prévoir des recours efficaces pour les contraventions à la présente loi.»⁹¹ L'objectif de cette loi est donc double : la protection des renseignements personnels sur la santé d'une part, y compris l'accès par le particulier, son droit de rectification et ses recours, et la fourniture efficace de soins de santé d'autre part. On touche dès lors le point crucial, qui est celui de l'équilibre à trouver entre ces deux aspects.

⁸⁴ *RJR-MACDONALD INC. c. CANADA* (Procureur général) [1995] 3 R.C.S. 199

⁸⁵ *Ibid.*, §32 :

« De toute évidence, la «santé» n'est pas un chef de compétence énuméré dans la *Loi constitutionnelle de 1867*. Comme le fait observer le juge Estey dans l'arrêt *Schneider c. La Reine*, [1982] 2 R.C.S. 112, à la page 142 :

« ... la «santé» n'est pas l'objet d'une attribution constitutionnelle spécifique, mais constitue plutôt un sujet indéterminé que les lois fédérales ou provinciales valides peuvent aborder selon la nature ou la portée du problème de santé en cause dans chaque cas. Vu que la santé comme matière constitutionnelle présente un caractère «informe» et qu'il s'ensuit que tant le Parlement que les législatures provinciales peuvent valablement légiférer dans ce domaine (...). »

⁸⁶ HEALTH INFORMATION ACT, R.S.A. 2000, c. H.5

⁸⁷ PERSONAL HEALTH INFORMATION ACT, S.M. 1997, c.51

⁸⁸ PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004, S.O. 2004, c.3, Sched. A

⁸⁹ SASKATCHEWAN HEALTH INFORMATION PROTECTION ACT (2003), c. H.O. 021

⁹⁰ E-HEALTH (Personal Health Information Access and Protection of Privacy) Act, S.B.C. 2008, c. 38

⁹¹ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ (L.O. 2004, c. 3), article 1.

L'article 4 de la LPRPS donne aux renseignements personnels sur la santé la définition qui suit :

« renseignements personnels sur la santé » : Sous réserve des paragraphes (3) et (4), s'entend de renseignements identificatoires concernant un particulier qui se présentent sous forme verbale ou autre forme consignée si, selon le cas : a) ils ont trait à la santé physique ou mentale du particulier, y compris aux antécédents de sa famille en matière de santé; b) ils ont trait à la fourniture de soins de santé au particulier, notamment à l'identification d'une personne comme fournisseur de soins de santé de ce dernier; c) ils constituent un programme de services au sens de la Loi de 1994 sur les soins de longue durée pour le particulier; d) ils ont trait aux paiements relatifs aux soins de santé fournis au particulier ou à son admissibilité à ces soins ou à cette assurance; e) ils ont trait au don, par le particulier, d'une partie de son corps ou d'une de ses substances corporelles ou découlent de l'analyse ou de l'examen d'une telle partie ou substance; f) ils sont le numéro de la carte Santé du particulier; g) ils permettent d'identifier le mandataire spécial d'un particulier.»⁹²

On constate que cette définition de renseignements personnels de santé est technologiquement neutre en ce qui a trait à la forme sous laquelle le renseignement est fourni ou consigné. La LPRPS va donc s'appliquer aussi bien au dossier papier qu'au dossier électronique ou à la transmission verbale. La définition du terme dossier dans la LPRPS vient confirmer l'approche technologiquement neutre que le législateur a choisi d'adopter.⁹³

Pour ce qui est des entités qui sont sujettes à l'application de la LPRPS, la Loi s'applique à tout « dépositaire de renseignement sur la santé »⁹⁴, soit : « une personne ou [...] organisation visée à l'une des dispositions suivantes qui a la garde ou le contrôle de renseignements personnels sur la santé par suite ou à l'égard de l'exercice de ses pouvoirs ou de ses fonctions ou de l'exécution du travail visé à la disposition. »⁹⁵ Suit une longue liste de personnes qui sont des dépositaires de renseignement sur la santé, tels que le praticien de la santé ou l'exploitant d'un cabinet ou groupe de praticiens de la santé, les fournisseurs de services, au sens de la Loi de 1994 sur les soins de longue durée, une société d'accès aux soins communautaires, un hôpital, un foyer de soins, une pharmacie, etc.

La LPRPS va donc encadrer de façon générale la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé, y compris les dossiers de santé, et ce, pour la majorité des praticiens du domaine de la santé. Il s'agit donc d'un régime uniforme applicable à la plupart des professionnels de la santé.

⁹² LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ (L.O. 2004, c. 3), article 4.

⁹³ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ (L.O. 2004, c. 3), article 2 : « Dossier de renseignements se présentant sous quelque forme ou sur quelque support que ce soit, notamment sous forme écrite, imprimée, photographique ou électronique. Sont toutefois exclus de la présente définition les programmes informatiques et autres mécanismes qui permettent de produire un dossier. »

⁹⁴ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ (L.O. 2004, c. 3), article 7

⁹⁵ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ (L.O. 2004, c. 3), article 3

e) Lois sur la protection des renseignements personnels au Québec

Richard Langelier rappelle que le Québec, dans les années 80, a fait un choix important, à savoir celui de « l'égale et universelle protection de tous les renseignements personnels. »⁹⁶ Vu les enjeux spécifiques des renseignements personnels sur la santé, l'approche québécoise qui traiterait de façon identique tous les types de renseignements personnels pourrait paraître quelque peu problématique.

Nous avons mentionné plus tôt l'existence au Québec d'une loi reconnue comme essentiellement similaire à la LPRPDE, à savoir la Loi sur la protection des renseignements personnels dans le secteur privé, qui vise à encadrer « l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil. »⁹⁷

Comme la LPRPS ontarienne, la Loi sur la protection des renseignements personnels dans le secteur privé est technologiquement neutre, s'appliquant aux « renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles »⁹⁸. Quant aux renseignements visés, il s'agit de « tout renseignement qui concerne une personne physique et permet de l'identifier. »⁹⁹ Soulignons que cette définition de renseignement personnel est la même que celle que l'on retrouve à l'article 54 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

La Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP), comme son nom le laisse entendre, n'est pas applicable au secteur public de la santé; sont explicitement exclus de son application les organismes publics tels que définis dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels¹⁰⁰. Cette dernière loi définit à son article 7 les établissements de santé¹⁰¹, en

⁹⁶ LANGEЛИER, Richard Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, Lex Electronica, vol. 9, été 2004, p. 2 [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009)

⁹⁷ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ, L.R.Q. c. P-39.1, article 1

⁹⁸ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ, L.R.Q. c. P-39.1

⁹⁹ LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ, L.R.Q. c. P-39.1, article 2

¹⁰⁰ LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (chapitre A-2.1), article 3: « « organismes publics » (...) le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires et les établissements de santé ou de services sociaux. »

¹⁰¹ LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (chapitre A-2.1), article 7 : « Les établissements de santé ou de services sociaux comprennent les établissements publics visés par la Loi sur les services de santé et les services sociaux (chapitre S-4.2), les établissements privés visés par cette loi qui fonctionnent en ayant recours à des sommes d'argent provenant du fonds consolidé du revenu, les agences visées par cette loi, la Corporation d'hébergement du Québec ainsi qu'un centre de communication santé visé par la Loi sur les services préhospitaliers d'urgence (chapitre S-6.2). Les établissements de santé ou de services sociaux comprennent également les établissements publics visés par la Loi sur les services de

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

procédant par renvoi à la Loi sur les services de santé et les services sociaux (chapitre S-4.2). On constate ici même une première complexification de la protection des renseignements personnels; en effet, il faut lire et maîtriser un nombre conséquent de lois afin de connaître les obligations respectives de chaque professionnel relativement aux renseignements personnels sur la santé.

La province du Québec a choisi d'instaurer des régimes d'exception dans un grand nombre de domaines afin que les renseignements personnels puissent circuler. Ainsi, le régime général de protection des renseignements personnels ne peut plus vraiment être considéré comme la norme de référence; il s'agit au contraire de l'exception, les régimes spéciaux et dérogatoires étant en quelque sorte devenus la norme.

Désormais, dans le régime juridique Québécois, le « régime de protection varie en fonction de la nature des renseignements en cause et de la personne qui en dispose. »¹⁰² Ainsi, un renseignement personnel donné, détenu par un membre d'un ordre professionnel sera régi par le Code des professions, par la LPRPSP s'il est détenu par une pharmacie privée, par la Loi médicale s'il est détenu par un médecin.

f) Lois relatives à la protection des renseignements personnels en Colombie-Britannique

La Colombie-Britannique, comme nous le mentionnions précédemment, dispose d'une loi sur la protection des renseignements personnels, le Personal Information Protection Act (PIPA), qui a été reconnue comme essentiellement similaire à la LPRPDE¹⁰³. On constate en effet que les objectifs des deux lois sont similaires¹⁰⁴; comme la LPRPDE, le PIPA vise à régir la collecte, l'utilisation, et la divulgation des renseignements personnels détenus par des organisations. Sont exclus les organismes publics, régis par le *Freedom of Information and Protection of Privacy Act* (R.S.B.C. 1996, c. 165) (ci-après FIPPA), qui énonce à son article 2 les objectifs de cette loi, qui vise expressément les « *public bodies* »¹⁰⁵. L'annexe 1 qui donne les définitions des termes utilisés dans le FIPPA, précise ce que sont les « *public bodies* »; il s'agit notamment de « *local public body* », qui comprend le « *health care body* », c'est-à-dire les hôpitaux et autres centres de soins, y compris les soins psychiatriques. En outre, il nous faut considérer la définition du terme « *record* », à savoir « *books, documents, maps, drawings, photographs,*

santé et les services sociaux pour les autochtones cris (chapitre S-5), les établissements privés visés par cette loi qui fonctionnent en ayant recours à des sommes d'argent provenant du fonds consolidé du revenu et les conseils régionaux de santé et de services sociaux institués en vertu de cette loi. »

¹⁰² LANGELIER, Richard Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, *Lex Electronica*, vol. été 2004, pp. 2 et 3 [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009)

¹⁰³ PERSONAL INFORMATION PROTECTION ACT, S.B.C. 2003, c. 63

¹⁰⁴ Lire l'article 2 de la PERSONAL INFORMATION PROTECTION ACT et l'article 3 la LPRPDE

¹⁰⁵ FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (R.S.B.C. 1996, c. 165), section 2 : « The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by

- (a) giving the public a right of access to records,
- (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
- (c) specifying limited exceptions to the rights of access,
- (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
- (e) providing for an independent review of decisions made under this Act. »

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records; (...)»¹⁰⁶ Les dispositions du FIPPA s'appliquent à tous les dossiers conservés par ou sous le contrôle d'un organisme public.¹⁰⁷ La définition de dossier, qui cite certains supports sur lesquels fixer l'information, reste suffisamment ouverte pour inclure toutes les formes actuelles de fixation de renseignements personnels. Quant à la définition de renseignement personnel, la même définition générique qui a été utilisée dans d'autres lois sur la protection des renseignements personnels a été adoptée.¹⁰⁸

De façon encore beaucoup plus spécifique, en ce qui a trait aux bases de données sur les renseignements personnels sur la santé, la Colombie-Britannique a promulgué le 29 mai 2008 le *E-Health (Personal Health Information Access and Protection of Privacy) Act* (ci-après *E-Health Act*). Cette loi vise à régir les conditions de collecte, d'utilisation et de divulgation des renseignements personnels sur la santé à travers les bases de données du secteur de la santé, et ce, dans le but de fournir des services de soins de santé aux individus, ou encore pour faciliter le travail de l'administration pour la facturation des services, pour répondre aux besoins des services de santé publics ou pour la recherche. Les renseignements personnels sur la santé sont définis comme suit : « recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual; (...) »¹⁰⁹

Cette loi répond à un besoin spécifique, soit la circulation de l'information. La numérisation des renseignements personnels sur la santé et leur dématérialisation a permis un accroissement de la circulation de l'information, qui voyage désormais à travers différents réseaux de la santé. Dès lors, il importe de conserver le fragile équilibre entre la protection des renseignements personnels et leur circulation en vue de la fourniture de soins à l'utilisateur.

4.2 FINALITÉ ET FONDEMENT DU CONSENTEMENT DE L'USAGER POUR LA COLLECTE, L'UTILISATION ET LA DIVULGATION DES RENSEIGNEMENTS PERSONNELS

De façon systématique, toutes les lois sur la protection des renseignements personnels canadiennes exigent, à un certain degré, le consentement préalable de l'utilisateur pour la collecte, l'utilisation et la divulgation des renseignements personnels. La LPRPDE, par exemple, pose comme règle générale l'obtention du consentement à l'article 4.3 de l'annexe 1, : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. » Des dispositions similaires se retrouvent à l'article 6 du PIPA, aux articles 6, 12, 13, et 15 de la LPRPSP, et aux articles 53 et 59 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ainsi qu'à l'article 29 de la LPRPS.

¹⁰⁶ FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (R.S.B.C. 1996, c. 165), schedule 1

¹⁰⁷ FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (R.S.B.C. 1996, c. 165), section 3 : « This Act applies to all records in the custody or under the control of a public body (...) »

¹⁰⁸ FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (R.S.B.C. 1996, c. 165), schedule 1 « « Personal information » means recorded information about an identifiable individual other than contact information; »

¹⁰⁹ E-HEALTH ACT, section 1

Ainsi, le consentement de celui que concernent lesdits renseignements est en principe à la base de tout le système de protection des renseignements personnels.¹¹⁰

Les renseignements personnels recueillis par le médecin sont souvent essentiels pour que le traitement approprié soit délivré au patient. Dans le cadre de cette relation entre le patient et son médecin, les renseignements personnels qui sont fournis appartiennent au patient, et cela même si le médecin les retranscrit dans un dossier. Le patient reste propriétaire des renseignements personnels alors même que le médecin est propriétaire du dossier. C'est ce qu'affirme la Cour suprême dans la décision *McInerney c. MacDonald* :

« Un médecin commence à constituer un dossier médical quand un patient choisit de lui faire partager des détails intimes sur sa vie pendant une consultation. Le patient "confie" ces renseignements personnels au médecin à des fins médicales. Il importe de ne pas oublier la nature de la relation médecin-patient dans le cadre de laquelle ces renseignements sont confiés. Dans l'arrêt Kenny c. Lockwood, [1932] O.R. 141 (C.A.), le juge Hodgins affirme, à la p. 155, que la relation entre le médecin et son patient en est une dans laquelle il faut faire "confiance" au médecin. Dans l'affaire Henderson c. Johnston, [1956] O.R. 789, ces propos ont été mentionnés et approuvés par le juge LeBel qui a lui-même qualifié la relation médecin-patient de [TRADUCTION] "fiduciaire et confidentielle"(...)»¹¹¹

La confiance du patient qui devra révéler au médecin des renseignements intimes repose sur sa foi que les renseignements personnels qui sont divulgués sont et demeureront confidentiels. On retrouve, au Québec, cette exigence de confidentialité des dossiers médicaux, et des renseignements personnels qui y apparaissent, aux articles 20 du Code de déontologie des médecins¹¹², à l'article 60.4 du Code des professions¹¹³, et également à l'article 42 de la Loi

¹¹⁰ L'importance du consentement préalable est reconnue depuis longtemps dans le domaine de la santé; en effet, le consentement aux soins de santé est primordial et se retrouve codifié dans plusieurs lois canadiennes, notamment la Loi de 1996 sur le consentement aux soins de santé. S'il n'y pas de consentement, il ne peut y avoir de traitement, sous réserve de certaines exceptions expressément prévues par la Loi. Le consentement est présent tout au long du processus médical. Lorsque le patient se rend chez son médecin, il lui communique des renseignements personnels sur sa santé. Le médecin, qui va retranscrire ces renseignements, que ce soit sur un dossier papier ou bien dans un dossier électronique, doit obtenir le consentement du patient pour ce simple acte de retranscription d'informations sur la santé de l'utilisateur.

¹¹¹ *MCINERNEY c. MACDONALD*, [1992] 2 R.C.S. 138

¹¹² CODE DE DÉONTOLOGIE DES MÉDECINS (code des professions L.R.Q., c. C-26, a. 87; 2001, c. 78, a.6), article 20: « Le médecin, aux fins de préserver le secret professionnel :

1. doit garder confidentiel ce qui est venu à sa connaissance dans l'exercice de sa profession ;
2. doit s'abstenir de tenir ou de participer à des conversations indiscrettes au sujet d'un patient ou des services qui lui sont rendus ou de révéler qu'une personne a fait appel à ses services ;
3. doit prendre les moyens raisonnables à l'égard des personnes qui collaborent avec lui pour que soit préservé le secret professionnel ;
4. ne doit pas faire usage de renseignements de nature confidentielle au préjudice d'un patient ;
5. ne peut divulguer les faits ou confidences dont il a eu personnellement connaissance, sauf lorsque le patient ou la loi l'y autorise, ou lorsqu'il y a une raison impérieuse et juste ayant trait à la santé ou la sécurité du patient ou de son entourage ;
6. ne peut révéler à l'entourage du patient un pronostic grave ou fatal si celui-ci le lui interdit. »

¹¹³ CODE DES PROFESSIONS (L.R.Q., c. C-26), article 60.4 : « Le professionnel doit respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession. »

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

médicale¹¹⁴. En résumé, la confidentialité, c'est le « maintien du secret des renseignements personnels une fois qu'ils ont été divulgués »¹¹⁵.

Certaines lois, comme la LPRPS, prévoient aussi bien le consentement tacite que le consentement exprès¹¹⁶. Ainsi, les renseignements personnels sur la santé pourront être divulgués à certaines personnes dans le cadre de la prestation de soins de santé, l'utilisateur étant considéré y avoir tacitement consenti. De façon générale, les renseignements personnels sur la santé circulent entre les différents intervenants de soins de santé, en vue de permettre au patient d'obtenir les soins dont il a besoin. Ainsi, nous retrouvons donc une exigence de consentement exprès lorsque les renseignements de santé sont divulgués à d'autres fins que celle de fournir des soins de santé. C'est le cas, par exemple, de renseignements qui seraient demandés par des assureurs, des employeurs, etc.

La LPRPS est encore plus précise sur le consentement, indiquant les éléments qui doivent être réunis pour l'obtention d'un consentement valide : le consentement doit être celui du particulier, il doit être éclairé, doit porter sur les renseignements et ne doit être obtenu ni par supercherie, ni par coercition¹¹⁷.

La Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives, Projet de loi 83, a ajouté en 2005 de nouvelles dispositions à la LSSSS¹¹⁸, afin d'y inclure des obligations d'information spécifiques relativement au dossier de santé du Québec¹¹⁹. L'article 19 de la Loi sur les services de santé et les services sociaux (LSSSS) précise que le consentement de l'utilisateur est nécessaire pour tout accès à ce dossier.¹²⁰ Plus important encore, le consentement est essentiel à la constitution même d'un dossier informatisé. Tout refus de consentir à l'établissement d'un tel dossier empêche les services de santé de le

¹¹⁴ LOI MÉDICALE (L.R.Q., chapitre M-9), article 42: « Un médecin ne peut être contraint de déclarer ce qui lui a été révélé à raison de son caractère professionnel. »

¹¹⁵ TREMBLAY, Geneviève « L'influence du droit constitutionnel à la vie privée dans le domaine de la télémédecine », 29 Queen's L. J. (2003) 326, 334

¹¹⁶ LPRPS, article 18(2) : « (2) Sous réserve du paragraphe (3), le consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé concernant un particulier peut être exprès ou implicite. 2004, chap. 3, annexe A, par. 18 (2). » Le consentement exprès est notamment requis dans les cas où le dépositaire des renseignements personnels souhaiterait utiliser ces renseignements personnels pour des fins commerciales (article 33) ou pour des fins de financement d'associations par exemple (article 32)

¹¹⁷ LPRPS, article 18(1)

¹¹⁸ La Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives, Projet de loi 83, a été adoptée le 25 novembre 2005 et sanctionnée le 30 novembre 2005. La Loi modifiant la Loi sur les services de santé et les services sociaux, la Loi sur l'assurance maladie et la Loi sur la Régie de l'assurance maladie du Québec, Projet de loi no 70, adoptée le 27 mai 2008 et sanctionnée le 28 mai 2008, est venue modifier à son tour certaines des dispositions qui avaient été ajoutées à la LSSSS en 2005. À ce jour, certaines de ces dispositions de la LSSSS qui ont été ajoutées ou modifiées par ces lois n'ont toujours pas été mises en vigueur (520.5 et suivants). Nous référerons directement, dans notre document, aux nouvelles dispositions de la LSSSS issues de ces lois modificatrices adoptées en 2005 et 2008.

¹¹⁹ LSSSS, article 520.14, alinéa 2 : « Les personnes appelées à manifester un tel consentement doivent préalablement être informées des objectifs et des finalités poursuivis et des modalités de fonctionnement concernant l'accès, l'utilisation, la communication, la conservation et la destruction des renseignements conservés conformément au présent titre. »

¹²⁰ LSSSS, article 19 : « Le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'utilisateur ou de la personne pouvant donner un consentement en son nom. »

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

créer.¹²¹ Le consentement peut être donné de façon verbale, mais il sera obligatoirement par écrit dans les cas où le consentement est demandé pour l'utilisation des renseignements personnels à des fins de recherche¹²²

La réglementation américaine du *Department of Health and Human Services* (ci-après HHS), faisant suite au *Health Insurance Portability and Accountability Act of 1996* (ci-après HIPAA), requiert dans certains cas des mesures pour l'obtention du consentement : « in plain language; inform individual that PHI (personal health information) may be used and disclosed to carry out treatment, payment, or health care operations; indicate that the individual can revoke the consent in writing; and request that the covered entity restrict how PHI is used or disclosed for health care purposes. »¹²³ Il faut souligner que le HIPAA n'impose qu'un cadre de protection minimal, puisque les États américains peuvent adopter des règles plus contraignantes relativement aux renseignements personnels. On remarque que la règle du consentement est quelque peu différente de ce que l'on retrouve au Canada, puisque la législation canadienne ne requiert pas le consentement pour les divulgations de renseignements personnels aux fins de traitement, paiement ou autres opérations en liens avec les soins de santé.¹²⁴ La particularité de cette réglementation américaine repose sur les demandes d'autorisation qui sont expressément requises pour l'utilisation et la divulgation de certains renseignements personnels de santé dans certaines circonstances prévues par la réglementation.¹²⁵ De plus, un formalisme particulier est exigé concernant ces demandes d'autorisation.¹²⁶

En France, outre les articles de la Constitution et du Code civil qui affirment le droit à la protection de la vie privée, on relèvera l'existence de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après Loi informatique et liberté), qui met en place

¹²¹ LSSSS, article 520.6

¹²² LSSSS, article 19.1

¹²³ 45 C.F.R §164.506, lire GOSTIN, Lawrence O. James G. Hodge, Jr., and Lauren Marks, The Nationalization of Health Information Privacy Protections, * Connecticut Insurance Law Journal, 283 2001-2002, 306.

¹²⁴ 45 C.F.R §164.506 (c)

¹²⁵ 45 C.F.R §164.508: « Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization. »

¹²⁶ 45 C.F.R §164.508(c)(1): « A valid authorization under this section must contain at least the following elements:

- (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- (iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- (iv) A description of each purpose of the requested use or disclosure. The statement ``at the request of the individual'' is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- (v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement ``end of the research study," none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
- (vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided. »

un système de déclaration et d'autorisation préalable pour le traitement de données à caractère personnel. Le chapitre 9 de cette loi vise tout particulièrement le traitement de données à caractère personnel ayant pour finalité la recherche dans le domaine de la santé. Mais d'autres lois viennent également insister sur la nécessité d'obtenir le consentement du patient : c'est ce que fait l'article L.1111-8, qui se trouve au chapitre I du Code de la santé publique : Information des usagers du système de santé et expression de leur volonté¹²⁷. Cet article est essentiel, puisqu'il fait mention de la Loi informatique et libertés, qui édicte les exigences relatives aux traitements automatisés de fichiers.

Si l'on s'intéresse aux modalités spécifiques du « dossier médical personnalisé » (ci-après DMP), on trouve la création de ce dossier médical personnel à l'article L. 1111-14 du Code de la santé publique, qui en précise l'objectif, et établit la nécessité que ce dossier soit détenu par un « hébergeur de données »¹²⁸ : « Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention. Ce dossier médical personnel est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8. » Précisions que des dispositions relatives à ce DMP figurent dans deux lois distinctes, l'une du 13 août 2004 relative à l'assurance maladie¹²⁹, et l'autre du 30 janvier 2007.¹³⁰

a) Remarques sur le consentement

Comme nous l'avons mentionné plus haut, le consentement éclairé de la personne à la collecte des renseignements personnels est généralement érigé en principe. Dans les faits, il sera pourtant plutôt rare que ce consentement soit véritablement éclairé. Par exemple, le patient qui consent, à sa première visite chez son médecin, à la collecte, à l'utilisation et à la divulgation de renseignements personnels aux fins de soin de santé ignore généralement que ce consentement permettra au médecin d'utiliser et de divulguer tous les autres renseignements

¹²⁷ CODE DE LA SANTÉ PUBLIQUE, article L.1111-8 : « Les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée.

Les traitements de données de santé à caractère personnel que nécessite l'hébergement prévu au premier alinéa, quel qu'en soit le support, papier ou informatique, doivent être réalisés dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La prestation d'hébergement, quel qu'en soit le support, fait l'objet d'un contrat. Lorsque cet hébergement est à l'initiative d'un professionnel de santé ou d'un établissement de santé, le contrat prévoit que l'hébergement des données, les modalités d'accès à celles-ci et leurs modalités de transmission sont subordonnées à l'accord de la personne concernée. (...) »

¹²⁸ *Ibid.*

¹²⁹ Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie

¹³⁰ Loi n°2007-127 du 30 janvier 2007 ratifiant l'ordonnance n°2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique (Titre résultant de la décision du Conseil constitutionnel n°2007-546 DC du 25 janvier 2007)

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

qui lui seront dévoilés dans le futur. En effet, le consentement n'est donné qu'une seule fois, et non à chaque visite chez le praticien.

Au Québec, le consentement est « implicite » pour tout ce qui touche le dossier de santé du Québec. Ce qui veut dire que le patient doit manifester son refus de consentir à la création d'un dossier de santé du Québec, à charge pour le médecin ou les autres praticiens qui peuvent créer ce dossier de santé du Québec d'aviser le patient qu'il lui est possible de refuser la création d'un tel dossier.

Toujours au Québec, on peut également se demander à quel point le consentement est libre. En effet si le patient refuse de donner son consentement, pourra-t-il bénéficier de tous les services de soins de santé? Sachant que la finalité déclarée, soit l'obtention des soins de santé, inclut tout le pan administratif de gestion de la santé, que ce soient les médicaments, ou les remboursements de soins de santé, celui qui refuse son consentement à l'utilisation et la divulgation des renseignements personnels aura-t-il les mêmes possibilités de prise en charge par le système des soins de santé?¹³¹ N'existe-t-il pas un risque de marginalisation des personnes qui refuseront de consentir à la collecte, l'utilisation et la divulgation des renseignements personnels de santé?

Le patient a un rôle actif à jouer dans le contrôle des accès au DSQ. En effet si le patient ne fait pas de demande d'accès à son dossier médical, il ignorera quels renseignements personnels sur sa santé pourront être utilisés et divulgués à d'autres personnes dans le cadre de la prestation des soins de santé. Certains patients, qui attacheraient peu d'importance à ces renseignements, peuvent choisir volontairement d'ignorer cette situation. Pour d'autres patients, ce n'est pas parce qu'ils attachent moins d'importance à ces renseignements qu'ils ignoreront cette situation, mais parce qu'ils n'auront pas été informés de l'existence de cette mesure permettant de contrôler l'accès au DSQ. À notre connaissance, le praticien qui recueille les renseignements personnels n'informe que très rarement, voire jamais, le patient qu'il pourrait transmettre des renseignements personnels sans son consentement. De plus, il existe un nombre effarant d'exceptions à la règle du consentement préalable pour l'utilisation et la divulgation des renseignements personnels.

b) Exceptions à l'exigence du consentement

Les nombreuses exceptions qui se retrouvent dans la quasi-totalité des juridictions étudiées, c'est à dire au Canada, aux États-Unis et, dans une moindre mesure, en France, sapent considérablement le principe fondateur du consentement préalable censé s'appliquer à la collecte, l'utilisation et la divulgation des renseignements personnels.

De façon générale, les exceptions, c'est-à-dire les cas où l'accès aux renseignements personnels sera permis sans consentement préalable, doivent être expressément prévues par la loi. On retrouve les exceptions qui permettent aux policiers ou autres corps chargés de faire respecter la loi d'avoir accès aux renseignements personnels de santé¹³²; les parents d'enfants en deçà d'un certain âge peuvent avoir accès aux renseignements personnels de santé de leur enfant¹³³; certaines autorités administratives de santé publique peuvent aussi se faire

¹³¹ Il faut noter qu'il est interdit de décliner d'octroyer des soins de santé sur la base d'un refus au consentement de la collecte, utilisation ou divulgation de renseignements personnels (voir par exemple: 45 C.F.R. §164.508(b)(4))

¹³² Aux États-Unis, il faut se référer à l'article 45 C.F.R. §164.512(f), intitulé Disclosures for law enforcement.

¹³³ LSSSS, article 21

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

transmettre des renseignements personnels¹³⁴; parfois les renseignements personnels peuvent être utilisés pour la recherche scientifique¹³⁵.

En Ontario, la LPRPS est limpide pour ce qui est des exceptions à l'exigence du consentement et élabore toutes les exceptions précitées. Ainsi, est permise la collecte directe¹³⁶ et indirecte de renseignements personnels. Cette collecte indirecte est permise lorsqu'il n'est pas raisonnablement possible de recueillir les renseignements auprès de la personne, et lorsque ces renseignements sont « raisonnablement nécessaires aux fins de la fourniture de soins de santé au particulier ».¹³⁷ Cette situation évoque immédiatement les cas d'urgence ou les cas où la personne souffre de troubles de la mémoire, par exemple. La collecte des renseignements personnels peut également être effectuée de façon indirecte pour des fins judiciaires¹³⁸. La loi peut également autoriser ou obliger la collecte de renseignements personnels¹³⁹ ou leur utilisation même sans le consentement du patient¹⁴⁰.

La LPRPS prévoit aussi des cas où l'utilisation des renseignements personnels sera permise sans le consentement du patient. Ainsi, le dépositaire de renseignements sur la santé peut utiliser ces renseignements pour la finalité prévue lors de la collecte du renseignement personnel, mais aussi pour toutes les autres fonctions qui sont raisonnablement nécessaires pour atteindre cette finalité.¹⁴¹ L'exemple donné par Speakman, Stoltz et Blake¹⁴² pour illustrer

¹³⁴ Aux États-Unis, il faut se référer à l'article 45 C.F.R. §164.512(e)

¹³⁵ Aux États-Unis, il faut se référer à l'article 45 C.F.R. §164.512(i)

¹³⁶ LPRPS Article 36(2): « Un dépositaire de renseignements sur la santé peut recueillir des renseignements personnels sur la santé directement auprès du particulier qu'ils concernent, même si celui-ci est incapable d'y consentir, si la collecte est raisonnablement nécessaire aux fins de la fourniture de soins de santé et qu'il n'est pas raisonnablement possible d'obtenir le consentement en temps opportun. 2004, chap. 3, annexe A, par. 36 (2). »

¹³⁷ LPRPS Article 36(1)b): « Un dépositaire de renseignements sur la santé peut recueillir indirectement des renseignements personnels sur la santé si, selon le cas : b) les renseignements visés sont raisonnablement nécessaires aux fins de la fourniture de soins de santé au particulier ou d'une aide à cet égard et il n'est pas raisonnablement possible de recueillir directement auprès de lui : (i) soit des renseignements personnels sur la santé raisonnablement exacts et complets, (ii) soit des renseignements personnels sur la santé en temps opportun; » Cependant, on peut s'interroger sur le fait que les renseignements personnels soient exacts et complets, rien ne garantit cette exactitude des renseignements personnels. En effet, les derniers renseignements personnels sur la santé d'une personne peuvent ne pas apparaître dans le dossier médical informatisé du patient. »

¹³⁸ LPRPS Article 36(1)c): « le dépositaire est une institution au sens de la *Loi sur l'accès à l'information et la protection de la vie privée* ou de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* ou agit en tant que partie intégrante d'une telle institution et il recueille les renseignements à une fin reliée : (i) soit à une enquête sur une violation d'un accord ou sur une contravention réelle ou prétendue aux lois de l'Ontario ou du Canada, (ii) soit à une instance poursuivie ou envisagée, (iii) soit à une fonction du dépositaire prévue par la loi; (...) »

¹³⁹ LPRPS Article 36(1)g): « le dépositaire recueille les renseignements auprès d'une personne que la loi ou un traité, un accord ou un arrangement conclu en vertu d'une loi ou d'une loi du Canada autorise ou oblige à les lui divulguer; (...) »

Article 36(1)h): « sous réserve des exigences et des restrictions, le cas échéant, qui sont prescrites, la loi ou un traité, un accord ou un arrangement conclu en vertu d'une loi ou d'une loi du Canada autorise ou oblige le dépositaire à recueillir les renseignements indirectement. 2004, chap. 3, annexe A, par. 36 (1); 2007, chap. 10, annexe H, art. 11. »

¹⁴⁰ LPRPS Article 37(1)b): « une fin à laquelle la présente loi, une autre loi ou une loi du Canada autorise ou oblige une personne à les divulguer au dépositaire; »

¹⁴¹ LPRPS Article 37(1) a): « (1) Un dépositaire de renseignements sur la santé peut utiliser des renseignements personnels sur la santé concernant un particulier à l'une ou l'autre des fins suivantes : a) la fin visée par leur collecte ou leur production et toutes les fonctions raisonnablement nécessaires à la

ce cas est celui de la vaccination des étudiants : lorsque l'information confirmant la vaccination a été collectée, elle pourrait être utilisée pour avertir les parents de la date de la prochaine vaccination. Les renseignements personnels peuvent également être utilisés sans le consentement du patient pour la gestion des risques ou des erreurs, et ce, afin d'améliorer la qualité des soins ou des programmes¹⁴³, la formation des personnels soignants¹⁴⁴, lorsque le dépositaire des renseignements personnels est partie ou témoin à une instance¹⁴⁵, pour le recouvrement des paiements de soins de santé¹⁴⁶, soit un éventail extrêmement large de besoins administratifs d'utilisation des renseignements personnels, ce qui ne sera pas sans risque pour la protection des renseignements personnels. L'utilisation des renseignements personnels de santé sans le consentement du patient est aussi permise aux fins de recherche¹⁴⁷. Comme dans le cas de la collecte sans consentement préalable, d'autres lois ou traités peuvent aussi autoriser l'utilisation des renseignements personnels sans le consentement du patient¹⁴⁸.

Dans le cas de la divulgation des renseignements personnels de santé du patient sans son consentement, nous atteignons le cœur même du difficile équilibre entre la protection de la vie privée du patient et le besoin de circulation de l'information sur la santé. Comme le soulignent Perun, Orr, et Dimitriadis: « The disclosure of personal health information permissible without consent in PHIPA [LPRPS] reflects the Act attempt to reconcile as much as possible patients' privacy interests, on the one hand, and the requirement to facilitate the effective provision of health care, on the other. »¹⁴⁹ La disposition centrale de la LPRPS se retrouve à l'article 6(3) : « La disposition de la présente loi qui autorise un dépositaire de renseignements sur la santé à divulguer des renseignements personnels sur la santé sans le consentement du particulier qu'ils concernent n'a pas pour effet : a) d'exiger que le dépositaire les divulgue, à moins que la loi ne l'y oblige; b) de soustraire le dépositaire à une exigence légale portant qu'il doit les divulguer; c) d'empêcher le dépositaire d'obtenir le consentement du particulier à la divulgation. » On constate que le dépositaire dispose d'un certain libre arbitre dans le choix de divulguer ou de ne pas divulguer les renseignements personnels, exception faite des cas où la loi exige la divulgation.

Néanmoins, il existe de nombreuses exceptions qui autorisent la divulgation des renseignements personnels sans le consentement du patient, notamment pour la recherche clinique¹⁵⁰, aux fins de mise à jour de registres¹⁵¹, pour la planification et la gestion du système de santé¹⁵², ou encore pour l'analyse du système de santé¹⁵³; dans ces derniers cas, toutefois, les données sont bien souvent anonymisées afin d'empêcher l'identification des personnes.

réalisation de cette fin, sauf s'ils ont été recueillis avec le consentement du particulier ou en vertu de l'alinéa 36 (1) b) et que celui-ci donne une consigne expresse à l'effet contraire; (...) »

¹⁴² SPEAKMAN Jane, Lori Stoltz, et Rod Blake, *Public Health Law and Practice in Ontario: Health Protection and Promotion Act*, Thomson Carswell, 2008, p. 214

¹⁴³ LPRPS article 37(1)d)

¹⁴⁴ LPRPS article 37(1)e)

¹⁴⁵ LPRPS article 37(1)h)

¹⁴⁶ LPRPS article 37(1)i)

¹⁴⁷ LPRPS article 37(1)j)

¹⁴⁸ LPRPS article 37(1)k)

¹⁴⁹ PERUN Halyna, Michael Orr, et Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act*, Irwin Law, Toronto, 2005 p. 347

¹⁵⁰ LPRPS article 44

¹⁵¹ LPRPS article 39(1)c)

¹⁵² LPRPS article 45

¹⁵³ LPRPS article 47

Finalement, une liste de cas où la divulgation sans consentement est permise apparaît aux articles 38 : pour la fourniture de soins de santé, 39 : aux fins des programmes de santé, 40 : lorsqu'un risque grave qui menace la santé ou la vie du patient nécessite la divulgation de ces renseignements, 41 : si une instance nécessite la divulgation de ces renseignements personnels, 42 : divulgation à la succession, 43 : cas de divulgation prévus par d'autres lois, 46 : aux fins de surveillance des paiements relatifs aux soins de santé.

Au Québec, l'article 19 de la LSSSS prévoit 11 exceptions à la règle de l'obligation du consentement à la communication de renseignements personnels, qui sont assez proches de celles que l'on retrouve à la LPRPS.¹⁵⁴ Mais il existe bien d'autres exceptions qui permettent la communication de renseignements personnels de santé. Selon Richard Langelier, il y aurait au Québec plus d'une centaine d'exceptions législatives ou jurisprudentielles permettant l'accès aux renseignements de santé¹⁵⁵.

¹⁵⁴ LSSSS article 19 : « Le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom. Un renseignement contenu au dossier d'un usager peut toutefois être communiqué sans son consentement: 1° sur l'ordre d'un tribunal ou d'un coroner dans l'exercice de ses fonctions; 2° à la demande du commissaire local aux plaintes et à la qualité des services en vertu de l'article 36, d'un médecin examinateur en vertu du troisième alinéa de l'article 47, d'un comité de révision visé à l'article 51 ou de l'un de ses membres en vertu du deuxième alinéa de l'article 55, d'un commissaire régional aux plaintes et à la qualité des services en vertu de l'article 69, d'un conseil des médecins, dentistes et pharmaciens ou d'un expert externe à l'établissement auquel ce conseil a recours en vertu du deuxième alinéa de l'article 214; 3° à la demande d'une personne qu'une agence désigne pour faire une inspection en vertu du deuxième alinéa de l'article 413.2 ou à la demande d'une agence ou d'une personne que celle-ci désigne pour faire une enquête en vertu du deuxième alinéa de l'article 414; 4° au ministre en vertu de l'article 433, pour l'exercice de ses fonctions prévues à l'article 431; 5° à une personne autorisée à faire une inspection en vertu du deuxième alinéa de l'article 489 ou de l'article 489.1; 6° à une personne désignée par le gouvernement en vertu du deuxième alinéa de l'article 500 et chargée d'enquêter sur une matière visée au premier alinéa de cet article; 7° dans les cas et pour les finalités prévus aux articles 19.0.1, 19.0.2, 19.0.3, 19.2 et 27.1, au deuxième alinéa des articles 78.1 et 107.1, au cinquième alinéa de l'article 108, au deuxième alinéa de l'article 185.1, à l'article 204.1, au quatrième alinéa de l'article 349.3, aux articles 520.3.0.1 et 520.3.1 et au premier alinéa de l'article 520.3.2; 8° à la demande, en vertu de l'article 77, de tout comité de révision visé à l'article 41 de la Loi sur l'assurance maladie (chapitre A-29) ou d'une personne ou d'un comité visé à l'article 192 du Code des professions (chapitre C-26), lorsque la communication du renseignement est nécessaire pour l'accomplissement de leurs fonctions; 9° dans le cas où le renseignement est communiqué pour l'application de la Loi sur la santé publique (chapitre S-2.2); 10° dans les cas et pour les finalités prévues aux articles 8 et 9 de la Loi visant à favoriser la protection des personnes à l'égard d'une activité impliquant des armes à feu (chapitre P-38.0001); 11° à toute personne ou tout organisme lorsque ce renseignement est détenu par un établissement qui exploite un centre de protection de l'enfance et de la jeunesse ou un centre de réadaptation et qu'il est nécessaire pour l'application de la Loi sur le système de justice pénale pour les adolescents (Lois du Canada, 2002, chapitre 1), pour la réadaptation ou la réinsertion sociale de cet usager ou en vue d'assurer la protection du public. »

¹⁵⁵ LANGEIER Richard, Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, *Lex Electronica*, vol. (été 2004, pp. 2-4) [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009). Voir également : LANGEIER Richard, et Jean Héту, L'accès à l'information et la protection des renseignements personnels: santé et services sociaux, Brossard, CCH, 2005; LECOURE Jean-François, Le dossier de l'usager: accès et communication des renseignements personnels, dans *Attention! Renseignements personnels en circulation...* 16^e Congrès Association sur l'Accès et la protection de l'information, Éditions Yvon Blais, 2008 p. 83

Cependant, le nouvel article 520.11 de la LSSSS mentionne clairement que les renseignements ne peuvent être communiqués par quiconque à des tiers, et ce, même avec le consentement de la personne concernée. L'interdiction est stricte et aucune exception n'est mentionnée. Toutefois, même si aucune exception n'est prévue pour le dossier de santé du Québec, celui-ci sera alimenté par les médecins qui, eux, disposent de dossier de l'utilisateur, pour lequel il existe de nombreuses exceptions à la règle du consentement préalable pour la collecte, l'utilisation et la divulgation des renseignements personnels.

Cependant dans le cas du dossier de santé du Québec, il semble que les renseignements ne pourront servir pour la recherche, et ce, même avec le consentement du patient puisque la recherche ne figure pas au titre des finalités permettant l'accès à ces renseignements, en vertu du nouvel article 520.5 de la LSSSS.

En Colombie-Britannique, il faut lire les articles 5¹⁵⁶, 8¹⁵⁷, 14¹⁵⁸, et 15¹⁵⁹ du *E-Health Act* pour trouver les cas où la divulgation des renseignements personnels est permise sans besoin de

¹⁵⁶ E-HEALTH, article 5 : « A designation order may authorize the disclosure of personal health information only for one or more of the following purposes: (a) if disclosure is inside Canada, a purpose set out in section 4 (a) to (f) [*collection and use of personal health information*]; (b) a planning or research purpose; (c) if disclosure is inside or outside Canada, a purpose set out in section 4 (i). »

¹⁵⁷ E-HEALTH, article 8 : « (1) Subject to subsection (3), the minister must in a designation order authorize a person whose personal health information is contained in the health information bank that is the subject of the designation order to make a disclosure directive. (2) An authorization under subsection (1) may limit the making of disclosure directives to (a) one or more types of personal health information, as identified in the designation order under section 3 (2) (a) [*establishment or designation of health information banks*], contained in the health information bank, (b) one or more purposes, as identified in the designation order under section 3 (2) (d), for which personal health information may be disclosed from the health information bank, and (c) one or more persons or classes of persons, as identified in the designation order under section 3 (2) (g). (3) Subsection (1) does not apply in respect of a health information bank if the data stewardship committee recommends to the minister that disclosure directives should not be made in respect of the health information bank. »

¹⁵⁸ E-HEALTH, article 14 : « (1) A person who requires information for a planning or research purpose may request information from a health information bank or ministry database only by submitting to the data stewardship committee (a) a request in the form and in the manner required by the data stewardship committee, and (b) information required by the data stewardship committee for the purposes of evaluating the request. (2) The data stewardship committee may approve the request if all of the following apply: (a) the request is for a planning or research purpose; (b) in the case of information from a health information bank, the disclosure is authorized under the terms of the designation order; (c) in the case of personal health information requested for a health research purpose, the requirements of section 15 [*disclosure for health research purposes*] have been met; (d) in the case of a request to disclose personal health information outside Canada, there is express consent, in writing, to the disclosure from each person who is the subject of the personal health information. (3) If the data stewardship committee approves the request, the administrator may, subject to any conditions set by the data stewardship committee on approving the request, disclose the information to the person who made the request. (4) An administrator must not disclose information under subsection (3) except under an information-sharing agreement (a) with the person who made the request, and (b) made, whether or not personal health information is disclosed, in accordance with section 19 (2) and (3) [*information-sharing agreements required for disclosure*]. »

¹⁵⁹ E-HEALTH, article 15 : « If a request for personal health information under section 14 [*disclosure for planning or research purposes*] is made for a health research purpose, the data stewardship committee may approve the request only if all of the following criteria are met: (a) the health research purpose cannot reasonably be accomplished unless personal health information is disclosed; (b) personal health information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the health research, unless the commissioner approves (i) the health research purpose, (ii)

consentement préalable du patient, qui sont plus limités qu'en Ontario et qu'au Québec. De plus, la loi prévoit une interdiction formelle de divulgation des renseignements personnels de santé pour des fins de recherche, à la différence du FIPPA, qui permet une telle divulgation, et des lois de l'Ontario et du Québec, qui permettent la divulgation à certaines conditions.¹⁶⁰

En France, l'article L. 1111-18 du Code de la santé publique interdit l'accès au dossier médical personnalisé (DMP) en dehors du cadre prévu aux articles L. 1111-15 et L. 1111-16, et ce, même si le patient donne son accord. Néanmoins, malgré cette interdiction générale, il existe des exceptions pour les cas où le patient ne serait pas en mesure de donner son consentement, autrement dit pour les cas d'urgence médicale¹⁶¹.

Force est de constater que, en matière de protection des renseignements personnels, le consentement du patient n'occupe plus, dans le domaine de la santé, le rôle central qui devrait lui revenir, étant bien souvent relégué à une simple question de forme. Les besoins de circulation de l'information de santé sont devenus si importants et si nombreux que toutes les exceptions qui prévoient la divulgation des renseignements personnels sans le consentement préalable tendent à donner à ce dernier un caractère facultatif plutôt qu'obligatoire.

De nombreux auteurs remettent en cause le consentement comme fondement des lois sur la protection des renseignements personnels, et ce, en termes plus qu'explicites : « [la] question du consentement, que certains invoquent comme un grand prêtre vaudou manipule ses amulettes, ne constitue qu'un hochet idéologique servant d'écran à une réalité beaucoup plus complexe et contradictoire.(...) Maintenir le consentement comme forme ou moyen ultime de protection des renseignements personnels relève de la mystification. »¹⁶²

Dans cette optique, une approche législative reposant sur le consentement comme base de protection des renseignements personnels n'est plus satisfaisante, comme le fait remarquer Langelier: « En fait, toutes les normes législatives actuelles s'appuient sur une approche en silo reposant sur la prémisse de la possession ou de la détention du renseignement personnel. Or, dans un réseau numérisé, ce n'est pas la logique de la possession, mais bien celle de l'accès, qui devient déterminante. »¹⁶³ De son côté, le professeur Trudel explique : « Pour l'information

the use of disclosed personal health information for the purpose of contacting a person to participate in the health research, and (iii) the manner in which contact is to be made, including the information to be made available to persons contacted; (c) any record linkage is not harmful to the individuals who are the subjects of the personal health information and the benefits to be derived from the record linkage are clearly in the public interest; (d) the data stewardship committee has imposed conditions relating to (i) security and confidentiality, (ii) the removal or destruction of individual identifiers at the earliest reasonable time, and (iii) the prohibition of any subsequent use or disclosure of personal health information without the express authorization of the data stewardship committee. »

¹⁶⁰ E-HEALTH, article 20 : « Despite this Act or the terms of a designation order, or section 35 of the *Freedom of Information and Protection of Privacy Act*, a person must not disclose (a) personal health information, or (b) information related to health service providers contained in a health information bank or ministry database for the purpose of market research. »

¹⁶¹ CODE DE LA SANTÉ PUBLIQUE, article L.1111-17

¹⁶² LANGELIER Richard, Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, *Lex Electronica*, vol. 9 été 2004, pp. 2-5 [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009)

¹⁶³ LANGELIER Richard, Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, *Lex Electronica*, vol. 9 été 2004, pp.2-4 [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009)

qui est nécessairement en possession des organisations de soins, le cadre juridique devrait s'attacher à en régir les conditions d'accès par chaque agent plutôt que d'en interdire la circulation. Dans un pareil contexte, l'enjeu n'est plus tellement de savoir si une information peut ou non être en possession de l'organisation ou de la personne soignante, mais plutôt si cette dernière a le droit d'y accéder et d'en faire usage pour prendre une décision dans une situation spécifique.»¹⁶⁴

4.3 ACCÈS AUX RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ

L'accès aux renseignements personnels doit être considéré d'un double point de vue : celui du patient et celui des professionnels de la santé. En effet, les lois prévoient en règle générale un accès pour le patient à ses renseignements personnels. Mais, avec l'arrivée des dossiers de santé électroniques, il est possible de contrôler de façon plus systématique les accès aux dossiers des patients par les professionnels de la santé. Ainsi, nous trouvons des dispositions spécifiques concernant la journalisation des accès et les profils d'accès des professionnels de la santé aux dossiers électroniques.

a) Accès par le patient à ses renseignements personnels

La Cour suprême, dans la décision *McInerney c. MacDonald*, a reconnu que le patient a le droit d'accéder à ses renseignements personnels¹⁶⁵. En outre, les lois qui encadrent la protection des renseignements personnels prévoient toutes un droit d'accès pour le patient, que ce soit la LPRPDE¹⁶⁶, la LPRPS¹⁶⁷, la LSSSS¹⁶⁸, ou encore le E-Health Act¹⁶⁹. Ce droit d'accès est également prévu à l'étranger, que ce soit aux États-Unis¹⁷⁰ ou en France¹⁷¹.

¹⁶⁴ TRUDEL Pierre, Gouvernance réseautique et effectivité des modes de protection des données personnelles dans les réseaux de cybersanté, dans *La Protection des données médicales- Les défis du XXI^e siècle*, sous la direction de Jean Herveg, Les éditions Thémis, Louvain-la-Neuve, 2008

¹⁶⁵ MCINERNEY C. MACDONALD, [1992] 2 R.C.S. 138 « Par conséquent, le patient a droit à un accès raisonnable lui permettant d'examiner les dossiers et d'en tirer des copies, pourvu qu'il paie un tarif légitime pour la préparation et la reproduction des renseignements. L'accès est limité aux renseignements que le médecin a obtenus en donnant un traitement. Il ne vise pas les renseignements obtenus en dehors de la relation médecin patient. »

¹⁶⁶ Annexe 1, neuvième principe- Accès aux renseignements personnels

¹⁶⁷ LPRPS article 1b)

¹⁶⁸ LSSSS article 17, et 520.21, voir également projet de loi 83.

¹⁶⁹ E-HEALTH ACT, article 17 (cet article n'est pas encore en vigueur, cependant nous pouvons trouver dans le projet de loi 24 l'énoncé de cet article: «One's own personal health information to be available 17 (1) Subject to this Act and the regulations made under it, an administrator must make available to a person

(a) that person's personal health information contained in the health information bank for which the administrator is responsible,

(b) a record of any disclosure directives made by the person that apply to the health information bank, and

(c) information respecting who has collected, used or disclosed that person's personal health information.

(2) Despite subsection (1), the administrator may deny, for any reason for which a person may be denied access to information under the *Freedom of Information and Protection of Privacy Act*, access to information or records described in subsection (1).

(3) Section 19 [information-sharing agreements] does not apply to disclosure of personal health information under this section.

¹⁷⁰ 45 C.F.R. §164.524 Access of individuals to protected health information

¹⁷¹ CODE DE LA SANTÉ PUBLIQUE, article L.1111-7

Il existe cependant des différences quant aux modalités d'accès au dossier. Par exemple, en Ontario la demande d'accès selon la LPRPS doit être faite par écrit¹⁷², tout comme aux États-Unis¹⁷³. Le Commissaire à la vie privée de l'Ontario, pour aider les patients à demander l'accès à leur dossier, met à disposition en ligne des formulaires à cet effet¹⁷⁴, alors qu'aux États-Unis ce sont des associations de défense des droits des patients, notamment, qui fournissent de tels formulaires¹⁷⁵. Dans le cas de l'Ontario, une exigence particulière est prévue à la Loi, qui est celle de s'assurer de l'identité de la personne qui fait la demande d'accès.¹⁷⁶ On pourra bien sûr s'interroger sur les moyens à mettre en œuvre pour obtenir une telle assurance. Exiger, par exemple, un numéro d'assurance maladie ou un autre numéro émis par l'administration et qui permet d'identifier une personne ne semble pas être une mesure très fiable s'il s'agit de vérifier avec certitude l'identité d'une personne.

Au Québec, des points de services médicaux permettront au patient d'accéder à son dossier. Il faut garder à l'esprit que, pour le moment, le dossier de santé du Québec n'en est qu'à la fin de sa phase d'expérimentation et n'est effectif que dans la région de Québec. Des dispositions de la LSSSS indiquent toutefois comment le patient pourra avoir accès aux renseignements consignés. Cet accès au dossier pourra également se faire à distance¹⁷⁷; des formulaires à cet effet sont mis en ligne à la disposition du public¹⁷⁸.

En France, le patient peut avoir accès, directement ou par l'intermédiaire de son médecin, aux renseignements sur la santé contenus dans son dossier médical personnel, les conditions d'accès étant prévues par voie réglementaire¹⁷⁹. L'article 43 de la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, précise que le patient a le choix quant à la forme que prendra l'accès aux données¹⁸⁰.

Pour ce qui est de la Colombie-Britannique, les informations sur les modalités d'accès ne sont pas encore disponibles, l'article permettant l'accès aux bases de données n'étant pas en vigueur.

Dans tous les cas étudiés, le patient qui souhaite obtenir une copie de son dossier devra assumer les frais reliés à la fourniture de la copie de son dossier. De plus, certaines législations, comme celles de l'Ontario¹⁸¹ et des États-Unis¹⁸², prévoient un délai de 30 jours

¹⁷² LPRPS, article 53(1)

¹⁷³ 45 C.F.R. §164.524(b)

¹⁷⁴ Formulaire en ligne à l'adresse: <http://www.ipc.on.ca/english/Resources/Forms/Forms-Summary/?id=209>

¹⁷⁵ Formulaire de l'association Privacy Patient right [En ligne] http://patientprivacyrights.org/media/Record_Request.pdf (page consultée le 13 septembre 2009)

¹⁷⁶ LPRPS, article 54(9)

¹⁷⁷ LSSSS, article 520.21

¹⁷⁸ Formulaire de demande d'accès au dossier de santé du Québec: <http://www.dossierdesante.gouv.qc.ca/download.php?f=279220f71ca10fc9d1ce3532e6ced1a0> (page consultée le 12 février 2010)

¹⁷⁹ CODE DE LA SANTÉ PUBLIQUE, article L.1111-7

¹⁸⁰ Article 43 de la LOI N°78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS : « Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de [l'article L. 1111-7](#) du code de la santé publique. »

¹⁸¹ LPRPS, article 52(6)(a)(b)

¹⁸² 45 C.F.R. §164.524(b)

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

pour la réponse à la demande d'accès. En France, le délai varie entre 48 heures et 8 jours pour l'accès au dossier, tandis qu'au Québec l'accès au dossier électronique se fait immédiatement au point de service.

Cependant, l'accès au dossier ne signifie pas pour autant que le patient sera en mesure de comprendre l'information qui lui sera communiquée. Dans ce sens, il faut reconnaître que le fait d'être assisté par un praticien, comme c'est le cas en France où ce devoir d'assistance est imposé, laisse présumer une meilleure compréhension de l'information médicale par le patient et dès lors, une plus grande accessibilité. Il faut noter qu'au Québec, l'article 25 de la LSSSS prévoit qu'un « établissement qui fournit à l'usager un renseignement de nature médicale ou sociale le concernant et contenu dans son dossier doit, à la demande de cet usager, lui procurer l'assistance d'un professionnel qualifié pour l'aider à comprendre ce renseignement ». Concernant le dossier de santé du Québec l'article 520.22, qui vient garantir le droit du patient d'obtenir sur demande l'assistance d'une personne ressource pour lui permettre de comprendre l'information qui figure dans son dossier.¹⁸³ Aucune obligation d'information du patient de l'existence d'une telle personne ressource n'a toutefois été prévue.

Aux États-Unis, l'article 164.524 (c)(2)(ii) du Code de réglementation fédérale mentionne expressément qu'une explication des informations peut être donnée au patient. À notre connaissance, il n'y a pas de telles mesures dans la LPRPS ontarienne, ni en Colombie-Britannique.

b) Exceptions au droit d'accès

Malgré le principe qui garantit l'accès du patient à son dossier, certaines exceptions relatives au droit d'accès aux renseignements personnels de santé sont expressément prévues par les différentes législations.

Ainsi au Québec s'il existe vraisemblablement un risque de préjudice grave pour la santé de l'usager en lui permettant d'avoir accès à son dossier médical, cet accès peut lui être refusé¹⁸⁴. On retrouve cette même exception en Ontario¹⁸⁵. Ne sont pas non plus accessibles au patient les renseignements qui figurent dans son dossier et qui ont été fournis par un tiers, s'ils sont susceptibles de permettre d'identifier ce tiers.¹⁸⁶

Certaines exceptions spécifiques sont prévues dans la réglementation américaine. Par exemple, le patient ne peut avoir accès aux données psychothérapiques¹⁸⁷. La LPRPS et la réglementation américaine partagent certaines exceptions. Par exemple ne seront pas accessibles au patient les renseignements qui portent sur la qualité des soins, ou ceux qui sont recueillis pour satisfaire les exigences d'un programme « d'assurance de la qualité ».¹⁸⁸

En cas de refus d'accès aux renseignements personnels, il existe dans presque tous les cas des procédures particulières pour permettre d'en appeler de la décision, que ce soit par le truchement d'un professionnel de la santé¹⁸⁹ ou du Commissaire à la vie privée provincial¹⁹⁰. Au

¹⁸³ LSSSS, article 189 et 520.22

¹⁸⁴ LSSSS, article 17

¹⁸⁵ LPRPS, article 52 (1)e)(i)

¹⁸⁶ LSSSS, article 18, également en Ontario article 52 (1)e)(iii)

¹⁸⁷ 45 C.F.R. §164.524(a)(1)(i)

¹⁸⁸ LPRPS article 51, et aux États-Unis 45 C.F.R. §164.524(a)(1)(ii),(iii) et suivants

¹⁸⁹ 45 C.F.R. §164.524(a)(3) et (4)

¹⁹⁰ LPRPS, article 54(8)

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

Québec, la LSSSS ne prévoit aucune disposition spécifique précisant l'organe auprès duquel il faut faire appel de la décision de refus. Cependant, une disposition de la LSSSS relative au dossier de l'utilisateur mentionne qu'en cas de refus d'accès à ses renseignements personnels, l'utilisateur peut se tourner, pour faire réviser la décision, vers un juge de la Cour supérieure ou de la Cour du Québec, ou vers la Commission d'accès à l'information.¹⁹¹

c) Accès contrôlé au dossier de santé électronique

Deux éléments semblent être essentiels pour garantir la confiance du patient relativement à l'informatisation croissante des dossiers de santé. D'abord, le patient doit être assuré que ses renseignements personnels sont confidentiels et qu'ils seront traités comme tels par le professionnel à qui il les confie. Ensuite, le patient doit pouvoir garder un certain contrôle sur ses renseignements personnels, ou à tout le moins sur l'accès à ces renseignements personnels.

Dans les faits, le patient n'a bien souvent aucune possibilité de contrôler qui a accès à son dossier de santé, dans la mesure où les profils d'accès et les droits conférés aux praticiens de la santé le sont par les gouvernements plutôt que par le patient lui-même¹⁹². Le patient, s'il souhaite participer à l'informatisation généralisée des dossiers de santé, se voit forcé d'accepter la règle du tout ou rien : soit il accepte que tous les professionnels de la santé qui y sont autorisés par le gouvernement aient accès aux dossiers de santé pour les finalités définies, soit il refuse, et, dans ce cas, il ne peut bénéficier des avancées que promet cette informatisation.

Le contrôle du patient sur les informations qui se retrouvent dans les dossiers de santé peut s'effectuer grâce à la possibilité, prévue à certaines lois, de verrouiller ou de masquer certaines informations, et par la capacité du patient à contrôler l'accès à son dossier de santé *a posteriori*.

d) Verrou ou masquage des informations

En vue de permettre au patient de conserver un certain contrôle sur ses renseignements personnels, la LPRPS a introduit un dispositif, surnommé « *lock box* », qui permet à l'utilisateur de refuser son consentement à la collecte, l'utilisation, ou la divulgation des renseignements personnels de santé pour des fins spécifiques, y compris les soins de santé, ou de le retirer (article 20(2) de la LPRPS). Ce mécanisme permet également à l'utilisateur de donner des instructions à la personne qui conserve les renseignements personnels de santé et cela dans certaines circonstances prévues aux articles 37(1)(a), 38(1)(a), et 50(1)(e) de la LPRPS. Perun, Orr, et Dimitriadis énoncent de façon explicite les objectifs visés par ces dispositions:

« The idea of the « lock box » stems from a fundamental privacy principle that patients should have a degree of control over the use and disclosure of their personal health information, whether before or after they have provided it to a health care provider. Enabling a patient to expressly withdraw or withhold consent to the sharing of personal health information in the delivery of health care, or to expressly state that information

¹⁹¹ LSSSS, article 27

¹⁹² LSSSS, articles 520.16 et 520.19, tel que modifiés par le projet de loi 70.

En France, l'accès aux données de santé est balisé par le décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le Code de la santé publique (dispositions réglementaires), articles R1110-1 et suivants du Code de la santé publique.

cannot be used or disclosed for such a purpose, gives the patient control over information about him or her.»¹⁹³

Cela dit, la *lock box* ontarienne n'est pas à toute épreuve. Nous avons mentionné plus haut plusieurs des exceptions à la règle du consentement préalable pour la collecte, l'utilisation et la divulgation des renseignements personnels. La *lock box* ne pourra évidemment agir comme verrou dans ces cas.

À l'opposé de ce que l'on observe en Ontario, le projet de dossier de santé Québec, s'il prévoit effectivement la possibilité de retirer son consentement à l'utilisation des renseignements qui apparaissent au dossier électronique¹⁹⁴, ne prévoit aucune mesure permettant de n'interdire la circulation que de certains des renseignements personnels de santé qui y figurent. C'était notamment l'une des critiques de la Commission d'accès à l'information lors des consultations sur le projet de loi 83 :

« si un patient ne veut pas que le professionnel de la santé transmette un renseignement précis le concernant à un service de conservation, devra-il (sic) obligatoirement révoquer un consentement préalablement donné pour que le renseignement ne soit pas communiqué? Par exemple, une personne qui ne souhaiterait pas que figure à son dossier régional le fait qu'on lui ait délivré un médicament pour combattre une maladie transmise sexuellement devra-t-elle révoquer son consentement pour éviter l'inscription de ce seul renseignement? »¹⁹⁵

En Colombie-Britannique, on trouve également, dans le *E-Health Act*, une mesure qui permet aux usagers d'empêcher la divulgation de certains renseignements personnels¹⁹⁶: « le ministre est tenu d'autoriser la soumission de « directives sur la divulgation » par les individus dont les renseignements médicaux sont enregistrés dans une base de données. Les patients peuvent ainsi limiter l'usage ou la divulgation de leurs renseignements médicaux personnels, en faisant masquer certaines informations afin qu'elles ne soient pas accessibles aux usagers du système.»¹⁹⁷ Cependant, « le ministre peut limiter l'application des directives de divulgation à un ou plusieurs types de renseignements, à une ou plusieurs fins, ou à une ou plusieurs catégories d'individus.»¹⁹⁸

En France, on étudie présentement des mesures identiques, soit la possibilité pour le patient de masquer certains renseignements personnels dans son dossier médical personnel.¹⁹⁹ Il ne fait

¹⁹³ Halyna Perun, Michael Orr, et Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act*, Irwin Law, Toronto, 2005 p. 284.

¹⁹⁴ LSSS, article 520.14

¹⁹⁵ COMMISSION D'ACCÈS À L'INFORMATION, *Mémoire sur le Projet de loi n°83, Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives*, Commission parlementaire des affaires sociales, janvier 2005 [En ligne] <http://www.bibliotheque.assnat.qc.ca/01/mono/2005/02/799301.pdf> (page consultée le 10 octobre 2009)

¹⁹⁶ E-HEALTH ACT, article 8(1)

¹⁹⁷ SYMINGTON Alison, La Colombie-Britannique adopte sa E-Health Act, *Revue VIH/SIDA, Droit et politiques*, Vol. 13, Numéro 2/3, Décembre 2008, p.15 [En ligne] <http://www.aidslaw.ca/publications/publicationsdocEN.php?ref=904> (page consultée le 10 novembre 2009)

¹⁹⁸ *Ibid.*

¹⁹⁹ CODE DE LA SANTÉ PUBLIQUE, article L.1111-21 alinéa 1: « Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé, fixe les conditions d'application des [articles L.1111-14 à L.1111-19](#) et notamment les

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

plus aucun doute, et ce, même si cette disposition n'apparaît ni dans le Code de la santé publique ni au Code de la sécurité sociale, que le patient disposera d'un droit de masquage de certains renseignements personnels²⁰⁰. La question qui a été longuement débattue est celle du droit de « masquer le masquage ». Finalement, le Parlement a décidé d'encadrer, par règlement, une telle procédure²⁰¹. Il faudra cependant, attendre un décret en Conseil d'État pour connaître « les conditions dans lesquelles certains renseignements peuvent être rendus inaccessibles par le titulaire du DMP »²⁰² tout comme les « modalités selon lesquelles le professionnel de santé accédant au DMP a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal. »²⁰³ En 2008, le ministre de la Justice a déclaré qu'il « s'agit de faire du DMP un dossier à la fois personnel pour le patient et partagé entre professionnels de santé. » « Personnel » car les patients disposeront ainsi d'un contrôle sur leurs propres données de santé. « Partagé », car le DMP est explicitement au service des professionnels de santé pour une meilleure coordination des soins. »²⁰⁴

Voilà bien, en résumé, les objectifs qui doivent sous-tendre la mise en place de tout dossier de santé électronique : contrôle du patient sur les données et circulation des informations pour coordonner les soins.

Les États-Unis ont également adopté des mesures qui permettent à l'utilisateur de restreindre la circulation des renseignements personnels.²⁰⁵ Ces mesures présentent toutefois un intérêt limité, puisque ces restrictions ne sont pas obligatoires, les organismes pouvant les refuser²⁰⁶.

e) Problématiques des *lock box* et autres mesures identiques

Ces *lock box* et autres mesures de masquage peuvent poser un problème aux praticiens, l'information figurant aux dossiers électroniques étant incomplète dès lors que le patient décide d'empêcher la divulgation de certains renseignements. Un patient qui cache à son médecin, par exemple, la prescription d'un médicament ne pourra limiter les risques d'une interaction médicamenteuse problématique. Or, l'un des objectifs de ces dossiers électroniques étant justement de réduire ce genre de risque, ses avantages s'en trouvent ainsi diminués.

En France, un rapport au ministre de la Santé et des Solidarités relativement au masquage d'informations par le patient dans son DMP précise que les risques liés à ce masquage sont

conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel, les conditions dans lesquelles certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical personnel ou son représentant légal ainsi que les modalités selon lesquelles le professionnel de santé accédant au dossier médical personnel a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal. » (nos soulignés)

²⁰⁰ MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux?

Médecine & Droit 2009 (2009) 24-41, 32

²⁰¹ LOI N°2007-1786 DU 19 DÉCEMBRE 2007 DE FINANCEMENT DE LA SÉCURITÉ SOCIALE POUR 2008, article 55

²⁰² MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux?

Médecine & Droit 2009 (2009) 24-41, 33

²⁰³ MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux?

Médecine & Droit 2009 (2009) 24-41, 33

²⁰⁴ MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux?

Médecine & Droit 2009 (2009) 24-41, 33

²⁰⁵ 5 CFR 164.522

²⁰⁶ 45 CFR 164.522 (a)(1)(ii)

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

essentiellement sanitaire²⁰⁷. Ce rapport argue que « la principale limite du droit au masquage est que le patient qui sait ce qu'il veut cacher ne sait pas forcément ce qu'il doit masquer. »²⁰⁸ Toutefois, le patient aura toujours la possibilité de demander à son médecin habituel de masquer les renseignements qui permettraient de connaître de façon indirecte l'information que le patient souhaite cacher.

f) Contrôle d'accès *a posteriori*

En France, l'article L. 1111-19 du Code de la santé publique instaure le « portail du dossier médical personnel »²⁰⁹. Ce portail, destiné notamment aux « bénéficiaires de l'assurance maladie », soit les usagers, et aux professionnels de santé, permet le « contrôle et la traçabilité des accès aux dossiers médicaux personnels »²¹⁰. L'utilisateur pourra, grâce à Internet, accéder au portail du dossier médical personnel et contrôler les éléments qui figurent dans son dossier, et il pourra voir les modifications qui y sont apportées. Ce système garantit un accès à tout moment au dossier médical personnel par le patient, renforçant ainsi sa confiance dans le système de soin de santé.

Au Québec, aucun portail n'a été prévu qui permettrait au patient d'accéder à son dossier ou à tout le moins d'avoir accès à l'information de journalisation²¹¹. L'accès au dossier est prévu à l'article 520.21 alinéa 3 de la LSSSS, qui précise: « L'agence ou l'établissement visé à l'article 520.7 doit également, à la demande de la personne concernée, l'informer du nom de l'intervenant qui a consulté les renseignements la concernant ou qui lui a transmis un renseignement, des coordonnées de cet intervenant ainsi que de la date de cette consultation ou de cette transmission. »²¹² En fait, lorsque l'utilisateur fait une demande d'accès à son dossier de santé, il peut également être informé des personnes qui ont eu accès à son dossier, mais cette procédure de demande d'accès sera le seul moyen à sa disposition pour contrôler les accès à son dossier.

En Ontario²¹³ et aux États-Unis²¹⁴, des systèmes ont été mis en place qui visent à avertir les usagers en cas d'accès non autorisé; rien de tel n'a été prévu au Québec²¹⁵.

²⁰⁷ RAPPORT AU MINISTRE DE LA SANTÉ ET DES SOLIDARITÉS, Le masquage d'informations par le patient dans son DMP, p. 8 [En ligne] <http://www.ladocumentationfrancaise.fr/rapports-publics/074000115/index.shtml> (page consultée le 15 novembre 2009)

²⁰⁸ RAPPORT AU MINISTRE DE LA SANTÉ ET DES SOLIDARITÉS, Le masquage d'informations par le patient dans son DMP, p. 9 [En ligne] <http://www.ladocumentationfrancaise.fr/rapports-publics/074000115/index.shtml> (page consultée le 15 novembre 2009)

²⁰⁹ CODE DE LA SANTÉ PUBLIQUE, article L.1111-19 alinéa 1 : « Il est institué un service unique d'accueil dématérialisé, dénommé "portail du dossier médical personnel", destiné aux bénéficiaires de l'assurance maladie et aux professionnels de santé. »

²¹⁰ CODE DE LA SANTÉ PUBLIQUE, article L.1111-19 alinéa 2 : « Ce portail assure des fonctions d'information générale et un service de gestion permettant aux bénéficiaires de l'assurance maladie de gérer leur dossier médical personnel et les droits d'accès des professionnels de santé. Il assure le contrôle et la traçabilité des accès aux dossiers médicaux personnels. Il produit les données de suivi d'activité nécessaires à l'évaluation de ce service. »

²¹¹ L'obligation de journalisation et de surveillance des accès se trouve à l'article 520.8 de la LSSSS, tel que modifié par le projet de loi 70.

²¹² LSSSS, article 520.21

²¹³ LPRPS, article 12 (2) : « Sous réserve du paragraphe (3) et des exceptions et exigences additionnelles, le cas échéant, qui sont prescrites, le dépositaire de renseignements sur la santé qui a la garde ou le contrôle de renseignements personnels sur la santé avise le particulier qu'ils concernent à la première occasion raisonnable en cas de vol ou de perte des renseignements ou d'accès à ceux-ci par des personnes non autorisées. 2004, chap. 3, annexe A, par. 12 (2). »

Selon les législations, on permet plus ou moins à l'utilisateur de contrôler les accès aux dossiers de santé. Soit l'utilisateur devra avoir un rôle actif en faisant des demandes d'accès à son dossier de santé pour y contrôler les accès passés, soit l'utilisateur est averti en cas d'accès non autorisé. Il nous semble que le système garantissant le plus grand contrôle est celui qui permet à la fois à l'utilisateur de contrôler en tout temps son dossier de santé électronique et qui prévoit des avis en cas d'accès non autorisé. Il paraît en effet peu probable que les utilisateurs vérifient de façon régulière leur dossier de santé; dans ces conditions il faut pouvoir prévenir les utilisateurs si un accès non autorisé au dossier de santé électronique s'est produit.

4.4 RISQUES D'ATTEINTE À LA VIE PRIVÉE RELATIFS AUX DOSSIERS DE SANTÉ ÉLECTRONIQUE

L'informatisation et la numérisation des dossiers de santé accroissent les risques d'atteinte à la vie privée liés à ces dossiers de santé. Les dossiers de santé papier comportaient déjà une part de risque, comme par exemple des accès non autorisés sans que le patient n'en soit informé. L'informatisation des dossiers offre l'avantage d'une plus grande facilité pour identifier les accès, les ajouts et retraits, etc. Il n'en demeure pas moins que des risques comme la perte ou le vol de dossiers, voire les utilisations secondaires des renseignements personnels de santé sont à prendre en considération avec l'implantation des dossiers de santé électronique.

Une note de recherche de la Chaire de recherche du Canada en sécurité, identité et technologie intitulée *La sécurité précaire des données personnelles en Amérique du Nord*²¹⁶ analyse notamment les incidents canadiens rapportés relativement à la sécurité de données personnelles. On y relève que, sur 23 incidents mentionnés au Canada, huit sont en lien avec le milieu de la santé. Les incidents rapportés sont liés soit à la négligence, au vol ou à la perte des données.

²¹⁴ 45 CFR 164.404 : « A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. » « Breach » étant défini à l'article 164.402: « means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. » (nos soulignés)

²¹⁵ LSSSS, article 520.23, tel que modifié par l'article 13 du projet de loi 70.

²¹⁶ DUPONT Benoît & Benoît GAGNON, *La sécurité précaire des données personnelles en Amérique du Nord*, Note de recherche n° 1, Chaire de recherche du Canada en sécurité, identité, et technologie, [En ligne] <http://www.benoitdupont.net/sites/default/files/securiteprecaire.pdf> (page consultée le 20 novembre 2009)

Les auteurs de la note de recherche soulignent que certains domaines sont particulièrement à risque en Amérique du Nord : la santé est le troisième secteur le plus touché par les incidents relatifs aux données personnelles. Les auteurs font part en ces termes de leurs inquiétudes :

« Ce constat est particulièrement problématique dans la perspective de la promotion qui est faite des services gouvernementaux en ligne (le e-government), puisque les services publics ne semblent pas en mesure de garantir l'intégrité des données personnelles et des transactions électroniques qui y sont associées. Dans la mesure où l'universalité d'accès aux services publics entraîne la création de fichiers qui regroupent des informations sur l'ensemble de la population, on peut aussi se poser la question de la prise de conscience au sein des administrations de l'intérêt que représente pour les fraudeurs l'accès à un tel gisement de données personnelles. Dans les deux cas, des investissements massifs devront être consentis au titre de la sécurité des données personnelles, aussi bien sur le plan des solutions technologiques que de la formation des fonctionnaires aux bonnes pratiques en ce domaine. »²¹⁷

Conscient de ces inquiétudes, la Commissaire à la vie privée de l'Ontario avait ordonné, en 2007, suite au vol d'un ordinateur portable contenant des renseignements personnels de santé, que les renseignements personnels de santé ne soient pas extraits des bases de données où ils étaient conservés, à moins qu'ils ne soient cryptés²¹⁸. Or, en 2009, une clé USB contenant des renseignements personnels sur des personnes en attente de vaccination contre la grippe H1N1 a été perdue. Contrairement à ce que la Commissaire à la vie privée de la Province avait ordonné en 2007, les renseignements personnels n'étaient pas cryptés²¹⁹.

La sécurité des données personnelles de santé est essentielle pour garantir la confidentialité de ces données. Attendu que la sécurité des données permet aux usagers d'avoir confiance dans le système de soins de santé, on ne peut que s'inquiéter de la survenance de tels événements en lien avec les renseignements personnels de santé.

²¹⁷ DUPONT Benoît & Benoît GAGNON, La sécurité précaire des données personnelles en Amérique du Nord, Note de recherche n°1, Chaire de recherche du Canada en sécurité, identité, et technologie, p. 9. [En ligne] <http://www.benoitdupont.net/sites/default/files/securiteprecaire.pdf> (page consultée le 20 novembre 2009)

²¹⁸ ORDER HO-004 de la Commissaire à la vie privée de l'Ontario, [En ligne] <http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7616> (page consultée le 20 novembre 2009)

²¹⁹ News Release, Commissioner Cavoukian expects health sector to encrypt all health information on mobile devices: Nothing short of this is acceptable [En ligne] <http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=917> (page consultée le 6 janvier 2010)

a) Identifiant unique comme moyen de dépersonnalisation des renseignements personnels

Au Québec, le nouvel article 520.9 de la LSSSS incorpore un nouvel élément, soit l'identifiant unique, dont on ne sait toutefois pas grand chose à l'heure actuelle. Cet identifiant unique sera notamment transmis à la RAMQ ainsi qu'aux établissements, aux agences et aux cabinets privés de professionnels de la santé. La Commission d'accès à l'information n'avait aucune information quant à cet identifiant lors des consultations parlementaires en 2005. Il en est toujours de même actuellement, à notre connaissance²²⁰.

Il faut comprendre qu'un identifiant unique peut être utile pour la circulation des informations dans les réseaux des services de santé. De plus, il s'agit d'une pratique plutôt répandue au sein de l'administration, puisqu'il existe déjà des identifiants comme les numéros de permis de conduire et le numéro d'assurance médicale.

Dans certains autres pays, en France²²¹ et aux États-Unis²²², par exemple, des identifiants uniques sont également utilisés ou prévus dans le domaine de la santé.

En France, ce nouvel identifiant unique pour l'accès au Dossier médical personnalisé s'appellera le « numéro d'identifiant santé ». À l'origine, on avait prévu d'utiliser à cette fin le numéro d'inscription au répertoire (NIR), plus connu en France sous le nom de numéro de sécurité sociale, qui présentait bien des avantages puisque « déjà existant comme identifiant unique de santé (...) simple, rapide à mettre en œuvre et évitait d'avoir à générer un nouvel identifiant pour les 60 millions de français. Le NIR constitue un numéro signifiant, unique, pérenne et fiable. »²²³ Cependant, et avec la bénédiction de la Commission nationale de l'informatique et des libertés²²⁴, ce numéro a été largement utilisé, et des risques de croisement et d'interconnexions de données ne sont pas à écarter. Un grand nombre de critiques se sont élevées contre l'utilisation de ce NIR, numéro facile à reconstituer, qui aurait permis bien trop aisément un accès au DMP par des tiers. Par la suite la CNIL s'est opposée à l'utilisation du NIR comme clé d'accès au DMP²²⁵. Finalement, un codage spécifique, le numéro d'identifiant santé, a été prévu à l'article L. 1111-8-1 du Code de la santé publique.²²⁶

²²⁰ COMMISSION D'ACCÈS À L'INFORMATION, Mémoire sur le Projet de loi n°83, Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives, Commission parlementaire des affaires sociales, janvier 2005 [En ligne] <http://www.bibliotheque.assnat.qc.ca/01/mono/2005/02/799301.pdf> (page consultée le 10 octobre 2009)

²²¹ Numéro d'identifiant santé ou NIS.

²²² SOBEL Richard, The demeaning of identity and personhood in national identifications systems, 15 Harvard Journal of Law & Technology 2002, p. 319

²²³ MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux? Médecine & Droit 2009 (2009) 24-41, 31

²²⁴ RECOMMANDATION DE LA CNIL DU 29 NOVEMBRE 1983

²²⁵ COMMUNIQUÉ DE PRESSE, CNIL, 20 FÉVRIER 2007

²²⁶ CODE DE LA SANTÉ PUBLIQUE, article L1111-8-1: « Un identifiant de santé des bénéficiaires de l'assurance maladie pris en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé défini à l'article L. 6321-1 est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé. Il est également utilisé pour l'ouverture et la tenue du dossier médical personnel institué par l'article L. 161-36-1 du code de la sécurité sociale et du dossier pharmaceutique institué par l'article L. 161-36-4-2 du même code. Un décret, pris après avis de la Commission nationale de l'informatique et des libertés, fixe le choix de cet identifiant ainsi que ses modalités d'utilisation. »

Aux États-Unis, le docteur Richard Sobel identifie les dangers reliés à cet identifiant unique et le risque de centralisation des informations. Un risque qui est notamment présent au Québec, puisque les informations seront centralisées de façon régionale. Le docteur Sobel relève notamment la possibilité d'accéder facilement aux bases de données médicales, et surtout les craintes vis-à-vis des atteintes à la confidentialité des renseignements²²⁷. Ces risques non négligeables sont de 4 ordres : accroissement des accès autorisés ou non autorisés aux informations par des tiers; utilisation subséquente de ces informations pour des finalités autres que celles indiquées lors de la collecte; possibilité d'utiliser cet identifiant afin de faire des recoupements de données; la confiance des usagers dans le système des soins santé pourrait être ébranlée.

La Commission d'accès à l'information appelle également à la vigilance avec cet identifiant unique, précisant qu'il existe un risque quant à l'utilisation de cet identifiant si l'on multiplie ses utilisations, puisqu'on facilite alors les recoupements d'informations. Une telle possibilité de recoupements simplifie de beaucoup la tâche qui consiste à dresser des profils sur les individus²²⁸, et de fichier ainsi la population.

b) Utilisations secondaires des renseignements personnels de santé

Le secrétaire du Département Américain de Santé et Services Humains a tenu à rappeler lors du dévoilement des règles du Code Fédéral : « Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions. »²²⁹

Nous avons eu l'occasion de préciser que les renseignements personnels de santé étaient collectés, utilisés et divulgués, de façon générale, pour permettre au patient d'obtenir des soins de santé : il s'agit de la finalité essentielle. Les dossiers de santé électroniques sont présentés comme une amélioration à la prise en charge des patients dans le système de santé, qui inclut un vaste volet administratif. Inforoute Santé du Canada, dans son livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable²³⁰, définit l'utilisation secondaire en ces termes : « l'utilisation et la divulgation de renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis initialement. »²³¹

²²⁷ SOBEL Richard, The demeaning of identity and personhood in national identifications systems, 15 Harvard Journal of Law & Technology 2002, p. 357 : « Yet the UHIDs would reduce medical privacy and confidentiality by making health information more easily available to employers, insurance companies, and law enforcement agencies that have access to the computer system. »

²²⁸ COMMISSION D'ACCÈS À L'INFORMATION, Mémoire sur le Projet de loi n°83, Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives, Commission parlementaire des affaires sociales, janvier 2005, p. 30 [En ligne] <http://www.bibliotheque.assnat.gc.ca/01/mono/2005/02/799301.pdf> (page consultée le 10 octobre 2009)

²²⁹ 65 Fed. Reg. 82,462; 82,467

²³⁰ INFOROUTE SANTÉ DU CANADA, livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable mars 2007 [En ligne] http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_FR.pdf (page consultée le 21 novembre 2009)

²³¹ INFOROUTE SANTÉ DU CANADA, livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable mars 2007, p.14 [En ligne] http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_FR.pdf (page consultée le 21 novembre 2009)

Inforoute Santé du Canada ajoute que : « malgré le fait que tous les renseignements du DSE seront initialement recueillis à des fins de traitement et de soins de santé ou à des fins d'administration du système de soins de santé, on peut raisonnablement s'attendre à ce qu'on ait intérêt, avec le temps, à accéder à ces renseignements à des fins secondaires comme la surveillance de la santé publique, l'analyse et la gestion du système de santé ainsi que la recherche. »²³² Cette utilisation des renseignements serait évidemment critiquable, dans la mesure où l'on s'écarterait ainsi de la finalité pour laquelle le patient consent à la collecte, l'utilisation et la divulgation de renseignements personnels.

Pour que soient permises ces utilisations secondaires, il serait indispensable que les renseignements personnels de santé soient dépersonnalisés ou anonymisés.²³³ Cependant la dépersonnalisation ou l'anonymisation n'écarte pas tous les risques, comme le démontre l'expérience de la professeure Latanya Sweeney²³⁴, qui a réussi à ré-identifier des personnes à partir d'informations anonymisées détenues par le Group Insurance Commission, responsable de l'assurance médicale des employés d'état. Cette société, croyant que les données étaient suffisamment anonymisées, en a fourni des copies à des chercheurs. La professeure Sweeney s'est procurée les renseignements contenus au registre électoral et a fait, à partir de certaines informations communes (code postal, date de naissance, sexe), une liaison entre les deux fichiers, qui lui a permis d'avoir accès aux renseignements contenus, par exemple, au dossier médical du gouverneur du Massachusetts. L'auteure s'est attardée à proposer certaines méthodes qui seraient susceptibles d'empêcher l'identification des personnes à partir de recoupement de fichiers et qu'il serait particulièrement pertinent de mettre en place dans l'éventualité où l'on déciderait de favoriser les utilisations secondaires.

Ainsi, la professeure Sweeney introduit la « k-anonymity » :

*« Often a data holder, such as a hospital or bank, needs to share person-specific records in such a way that the identities of the individuals who are the subjects of the data cannot be determined. One way to achieve this is to have the released records adhere to k-anonymity, which means each released record has at least (k-1) other records in the release whose values are indistinct over those fields that appear in external data. So, k-anonymity provides privacy protection by guaranteeing that each released record will relate to at least k individuals even if the records are directly linked to external information. »*²³⁵

²³² INFOROUTE SANTÉ DU CANADA, livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable mars 2007, p. 15 [En ligne] http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_FR.pdf (page consultée le 21 novembre 2009)

²³³ INFOROUTE SANTÉ DU CANADA, livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable mars 2007, p.15 [En ligne] http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_FR.pdf (page consultée le 21 novembre 2009)

²³⁴ SWEENEY Latanya, « K-Anonymity: A model for protection privacy » International Journal on Uncertainty, Fuzziness and knowledge-based Systems, 10 (5), 2002

²³⁵ SWEENEY Latanya, Achieving k-Anonymity Privacy Protection using Generalization and Suppression, [En ligne] <http://privacy.cs.cmu.edu/dataprivacy/projects/kanonymity/kanonymity2.html> (page consultée le 10 décembre 2009)

Au-delà des utilisations secondaires mentionnées plus haut, d'autres sont à prévoir. En effet, certaines personnes souhaiteraient certainement avoir accès aux données contenues aux dossiers de santé électroniques; on pense notamment aux assureurs ou même aux employeurs. D'ailleurs, concernant les assureurs, une décision de la Cour suprême dans l'affaire Frenette précise que le droit à la confidentialité n'est pas un droit absolu, mais bien un droit relatif, auquel on peut renoncer pour permettre aux assureurs d'accéder aux renseignements contenus dans un dossier médical, et ce, même si la finalité première pour laquelle les renseignements avaient été communiqués était l'octroi de soins de santé :

« Puisque le droit à la confidentialité jouit maintenant d'une protection quasi constitutionnelle au Québec, la question qui se pose est donc de savoir quelle est l'étendue de cette protection, spécialement en présence d'une renonciation expresse à ce droit. S'agit-il d'un droit absolu auquel on ne puisse déroger que dans des circonstances très exceptionnelles? Ou s'agit-il plutôt d'un droit relatif? Bien que, de prime abord, le grand principe général énoncé au premier alinéa de l'art. 9 de la Charte semble indiquer que l'on devrait favoriser une interprétation absolue, le droit d'une personne à la confidentialité de ses dossiers médicaux et l'obligation correspondante imposée à ceux qui en ont la possession revêtent un caractère indubitablement relatif. En fait, ceci est expressément reconnu au deuxième alinéa de l'art. 9 de la Charte elle-même, qui traite de l'obligation de respecter le secret professionnel. Le législateur a donc prévu, d'une part, que le titulaire du droit peut, de son propre chef, relever le professionnel de son obligation ou, d'autre part, que le législateur lui-même peut le faire dans l'intérêt public général au moyen d'une disposition expresse de la loi. Le fait que le législateur n'ait pas entendu faire du droit à la non-divulgence de documents confidentiels un droit absolu ou quasi absolu en l'insérant dans la Charte ressort également de la Loi sur les services de santé et les services sociaux qui régit l'obligation qu'ont les établissements de santé publics de garder confidentiels les dossiers des bénéficiaires de leurs services, notamment en vertu de l'art. 7 de cette loi, qui s'applique en l'espèce. »²³⁶

Dernièrement la Cour suprême, par le biais d'un *obiter dictum* dans la décision R.c.Patrick, est venue refermer quelque peu la porte qu'ouvrait la décision précitée aux utilisations secondaires des renseignements portant sur la santé :

« La Criminal Lawyers' Association cherche à rendre applicable à la collecte d'ordures la thèse selon laquelle des renseignements privés ne devraient rester connus que des personnes (en l'occurrence les éboueurs) à qui on entendait les communiquer, et qu'ils ne devraient être utilisés qu'aux fins pour lesquelles ils ont été communiqués, citant R. c. Mills, [1999] 3 R.C.S. 668, par. 108, et Dymnt, p. 431 432. On peut facilement accepter cette thèse dans le contexte, par exemple, de la relation entre le médecin et son patient. »²³⁷

On constate donc que la Cour suprême prend pour acquis le bien fondé du principe qui veut que, en matière de santé, l'utilisation des renseignements personnels soit liée à la finalité pour laquelle ils ont été initialement communiqués. Il faudra cependant suivre les prochaines décisions de la Cour suprême pour véritablement connaître ses intentions sur la question spécifique des utilisations secondaires.

²³⁶ FRENETTE c. MÉTROPOLITAINE (LA), CIE D'ASSURANCE VIE, [1992] 1 R.C.S. 647

²³⁷ R. c. PATRICK, 2009 CSC 17, [2009] 1 R.C.S. 579, au paragraphe 67

4.5 CAPACITÉ DES LOIS À RÉPONDRE AUX PROBLÉMATIQUES

Si l'on revient aux risques d'utilisation secondaire, il faut savoir que certaines lois, comme celles du Québec, et de la France, ont exclu la possibilité d'utilisation secondaire. En effet, en France, l'article L. 1111-18 du Code de la santé publique, ainsi que l'article L.161-36-3 de la Loi de 2007 précisent qu'aucun accès au DMP n'est permis en dehors des cas prévus par la loi, et ce, même avec l'accord de la personne concernée, accord que la loi interdit d'exiger. L'article est extrêmement précis sur ces points :

« L'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus aux articles L. 1111-15 et L. 1111-16, même avec l'accord de la personne concernée.

L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.

Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail. »²³⁸

Cette disposition empêche toute utilisation secondaire des renseignements personnels de santé contenus dans le DMP, que ce soit par les assureurs ou les employeurs qui, dans le cadre d'un contrat, désireraient évaluer l'état de santé de leur co-contractant, puisque ces dossiers leur sont inaccessibles.

Les sanctions en cas d'accès non autorisés sont prévues à l'alinéa 4 de l'article L. 1111-18 du Code de la santé publique, par renvoi à l'article 226-13 du Code pénal, qui impose un an d'emprisonnement et 15000 euros d'amende (environ 20 000 dollars).

Si l'on souhaite faire respecter le principe de confidentialité des renseignements personnels, il faut bien entendu que les sanctions prévues en cas de violation soient à la mesure du caractère extrêmement confidentiel des renseignements personnels de santé. Ainsi, il faut savoir que, en France, les hébergeurs de données de santé ainsi que les personnes qui travaillent pour leur compte sont nécessairement tenus au secret professionnel. En cas de violation du secret, les peines prévues à l'article L. 161-36-3 du Code de la sécurité sociale, tel que modifié par la Loi de 2007, imposent une peine d'emprisonnement d'un an et 150000 euros d'amende. Une cession des données de santé identifiantes, directement ou indirectement, à titre onéreux, et ce, même avec l'accord de la personne concernée, est susceptible d'entraîner la peine prévue à l'article 226-21 du Code pénal, soit cinq ans d'emprisonnement et 300 000 euros d'amende (plus de 420 000 dollars).²³⁹

²³⁸ Code de la santé publique. article L.111-18

²³⁹ MANAOUIL Cécile, Le dossier médical personnel (DMP): « autopsie » d'un projet ambitieux? Médecine & Droit 2009 (2009) 24-41, 29

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

En Colombie-Britannique, les amendes en cas de divulgation ou d'utilisation non autorisées peuvent atteindre 200 000 dollars.²⁴⁰

La LPRPS, en Ontario, prévoit également des amendes conséquentes, soit entre 50 000 et 250 000 dollars²⁴¹, et énumère à l'article 72(1) une longue liste d'infractions, notamment pour les cas de divulgation ou d'utilisation non autorisés par la LPRPS²⁴². Il faut également noter que le patient peut porter plainte auprès du Commissaire à la vie privée de l'Ontario, s'il croit qu'une personne a contrevenu à une disposition de la LPRPS²⁴³. La LPRPS prévoit également la possibilité d'octroi de dommages moraux, qui peuvent atteindre 10 000 dollars, à la victime d'une atteinte à la vie privée²⁴⁴.

²⁴⁰ E-HEALTH ACT, article 24: « (1) A person who contravenes any of the following sections commits an offence and is liable to a fine of up to \$200 000:

- (a) section 10 [*effect of disclosure directives*];
- (b) section 20 [*no disclosure for market research purposes*];
- (c) section 21 [*protection of privacy*];
- (d) section 22 [*whistle-blower protection*]. »

²⁴¹ LPRPS, article 72(2)

²⁴² LPRPS, article 72(1): «(1) Est coupable d'une infraction quiconque, selon le cas :

- a) recueille, utilise ou divulgue volontairement des renseignements personnels sur la santé contrairement à la présente loi ou à ses règlements d'application;
- b) présente sous de faux prétexte en vertu de la présente loi une demande d'accès à un dossier de renseignements personnels ou de rectification d'un tel dossier;
- c) relativement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé, ou à l'accès à un dossier de tels renseignements, fait une affirmation qu'il sait n'être pas véridique et portant que, selon le cas :
 - (i) il a le droit de consentir à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé concernant un autre particulier,
 - (ii) il satisfait aux exigences des alinéas 26 (2) b) et c),
 - (iii) il croit ce qui est énoncé au paragraphe 26 (5),
 - (iv) il a le droit d'avoir accès à un dossier de renseignements personnels sur la santé en vertu de l'article 52;
- d) élimine un dossier de renseignements personnels sur la santé dont le dépositaire a la garde ou le contrôle dans l'intention de se soustraire à une demande d'accès au dossier que celui-ci a reçue en vertu du paragraphe 53 (1);
- e) élimine volontairement un dossier de renseignements personnels sur la santé en contravention à l'article 13;
- f) contrevient au paragraphe 34 (2), (3) ou (4) ou à l'alinéa 47 (15) a), e) ou f);
- g) entrave volontairement le commissaire ou une personne que l'on sait agir sous son autorité dans l'exercice des fonctions que lui attribue la présente loi;
- h) fait volontairement une fausse déclaration afin d'induire ou de tenter d'induire en erreur le commissaire ou une personne que l'on sait agir sous son autorité dans l'exercice des fonctions que lui attribue la présente loi;
- i) omet volontairement de se conformer à une ordonnance rendue par le commissaire ou par une personne que l'on sait agir sous son autorité en vertu de la présente loi;
- j) contrevient à l'article 70. »

²⁴³ LPRPS, article 56(1)

²⁴⁴ LPRPS, article 65(3)

Aux États-Unis, la réglementation est excessivement exigeante pour ce qui est des mesures à mettre en place pour assurer la sécurité des renseignements personnels. Mentionnons à ce titre les articles 164.306, 308, 310, 312, et 314, relatifs aux standards de sécurité, aux mesures administratives de sécurité, aux mesures physiques de sécurité, ainsi qu'aux mesures techniques et organisationnelles. Concernant la règle générale de sécurité qui figure dans la réglementation américaine²⁴⁵, on peut constater une certaine similitude avec la formulation de la règle telle qu'on la retrouve dans la LPRPS²⁴⁶. Toutefois, la réglementation américaine est beaucoup plus précise, puisque certains facteurs doivent être pris en considération pour la mise en place des mesures de sécurité²⁴⁷. Au plan administratif²⁴⁸, la réglementation américaine exige que soient mises en œuvre des politiques et des procédures pour prévenir, détecter, limiter, et corriger les brèches de sécurité; des mesures comme l'analyse ou la gestion de risque sont préconisées. La réglementation américaine, très détaillée, fait figure de modèle.

En Ontario, la Commissaire à la vie privée a établi un guide relatif à la LPRPS afin d'aider les praticiens à se conformer aux nouvelles exigences légales.²⁴⁹

Au Québec, le nouvel article 520.13 à la LSSSS interdit expressément aux assureurs et employeurs l'accès aux renseignements contenus dans les dossiers de santé du Québec, et ce même avec le consentement de l'utilisateur.²⁵⁰ Il s'agit selon nous d'une interdiction absolue, qui referme la porte qui pouvait sembler avoir été ouverte précédemment par la Cour suprême (voir plus haut les commentaires sur l'affaire Frenette). Cependant, le médecin qui travaille pour un assureur pourra pour sa part avoir accès à un dossier de santé Québec.

²⁴⁵ 45 CFR 164.306(b)(1) « Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. »

²⁴⁶ LPRPS, article 12: « Un dépositaire de renseignements sur la santé prend des mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé dont il a la garde ou le contrôle soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée. »

²⁴⁷ 45 CFR 164.306(b)(2) In deciding which security measures to use, a covered entity must take into account the following factors:

- (i) The size, complexity, and capabilities of the covered entity.
- (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
- (iii) The costs of security measures.
- (iv) The probability and criticality of potential risks to electronic protected health information. »

²⁴⁸ 45 CFR 164.308

²⁴⁹ A GUIDE TO THE PERSONAL HEALTH INFORMATION PROTECTION ACT, December 2004, Information and Privacy Commissioner, Ontario, Canada [En ligne]
<http://www.ipc.on.ca/images/Resources/hguide-e.pdf> (page consultée le 30 novembre 2009)

²⁵⁰ LSSSS, article 520.13:

« Même avec le consentement de la personne concernée, il est interdit :

1° à un intervenant qui pratique dans un domaine où il ne rend pas à une personne des services de santé ou qui exerce, à l'égard d'une personne, des fonctions reliées aux domaines du contrôle ou de l'expertise ainsi qu'à un assureur et à un employeur de demander, d'exiger ou de recevoir de quiconque un extrait ou une copie d'un renseignement conservé par une agence ou par un établissement autorisé conformément au présent titre ;

2° à quiconque d'avoir accès de quelque manière à ces renseignements ou à un extrait ou à une copie de tels renseignements, pour la conclusion de tout contrat exigeant l'évaluation de l'état de santé d'une personne, tel un contrat d'assurance de personne ou un contrat d'embauche ou en cours d'emploi, ni à aucun moment ou à aucune occasion de son application. »

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

L'usager québécois dispose de plusieurs recours, auprès, notamment, du directeur des services professionnels²⁵¹, du Ministre²⁵² et de la Commission d'accès à l'information²⁵³. Concernant les sanctions prévues dans la LSSSS, Me Annette Lefebvre mentionnait lors d'une présentation faite à l'occasion d'une conférence de l'Institut canadien intitulée *La gestion et la protection des renseignements confidentiels dans le domaine de la santé et des services sociaux* que les risques qu'un établissement puisse faire face à des sanctions administratives et civiles sont minimes. Ce faible risque tient au fait que le patient va bien souvent ignorer le bris de confidentialité, puisqu'il n'y a aucune obligation de divulgation de tels événements. Quant à d'éventuelles poursuites civiles, elles seraient très rares, vu la nécessité pour le requérant d'établir la preuve prépondérante d'une faute, d'un préjudice et d'un lien de causalité entre la faute et le préjudice.

Concernant les amendes, il faut reconnaître que celles qui sont prévues dans la LSSSS sont en deçà de celles que l'on retrouve dans les autres législations examinées, et qu'elles sont loin de présenter le caractère dissuasif nécessaire à ce genre de peines : elles vont, pour une personne physique, de 6000 à 30 000 dollars, et, pour une personne morale, de 12 000 à 60 000 dollars. La confiance de l'usager dans le système des soins de santé risque malheureusement d'être ébranlée s'il constate que les sanctions que risque de se voir imposer le praticien en cas de violation ne sont que symboliques.

²⁵¹ LSSS, article 520.6 8^o paragraphe.

²⁵² LSSS, article 520.31

²⁵³ LSSS, article 520.30

5. CONCLUSION

L'informatisation des dossiers de santé pose un véritable défi tant sur le plan logistique que sur le plan législatif. Comparativement à ce qui pourra ressembler au Québec à un casse-tête juridique, l'approche ontarienne a le mérite de clarifier les règles pour la protection des renseignements personnels dans le secteur de la santé. Assujettir toutes les personnes qui traitent des renseignements personnels sur la santé à un régime unique simplifié en effet de beaucoup la gestion de tels renseignements. À défaut d'une loi unique, un code de la santé permettrait aussi de clarifier le système actuel, qui repose sur de multiples lois éparpillées.

Bien que les lois étudiées aient, de façon générale, les mêmes exigences concernant la protection des renseignements personnels, à savoir que le consentement préalable des usagers est nécessaire pour la collecte, l'utilisation ou la divulgation de renseignements personnels, il n'en demeure pas moins que le consentement, tel que prévu actuellement avec les finalités identifiées dans les lois étudiées, ne peut plus être considéré comme l'élément fondamental dans la protection des renseignements personnels. Il s'agit tout au plus d'une condition de forme qui procure au patient une apparence de contrôle sur ses renseignements personnels, en lui faisant croire qu'il lui est toujours loisible de refuser de consentir, ce qui n'est véritablement plus le cas.²⁵⁴

Même dans les cas où le patient refuserait d'y consentir, certaines lois prévoient des exceptions à l'exigence du consentement préalable, qui permettraient malgré tout la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé. Le trop grand nombre d'exceptions à la règle du consentement a affaibli la valeur de ce qui était le principe fondamental en matière de protection des renseignements personnels. En outre, les finalités telles qu'identifiées visent de plus en plus la collecte, la divulgation et l'utilisation des renseignements personnels pour des fins administratives périphériques à l'octroi de soins de santé. Il devient donc de plus en plus nécessaire d'informer les usagers des finalités de la collecte, de l'utilisation ou de la divulgation des renseignements personnels. Toutefois le non respect de cette obligation n'est bien souvent pas sanctionné.

L'étude nous a également permis de constater que certains outils, tel qu'un portail d'accès aux dossiers de santé électroniques peut être une solution innovante, qui permettrait véritablement aux usagers de contrôler les accès aux dossiers de santé électronique, ainsi que la possibilité de masquer certaines informations. Cette possibilité de masquer ou de bloquer certaines informations a été prévue dans plusieurs des législations examinées; cependant si, comme dans le cas pour le consentement, les exceptions sont trop nombreuses, alors l'efficacité d'une telle mesure sera anéantie. Il nous semble essentiel que l'utilisateur soit partie prenante de ces projets d'informatisation. Il s'agit de renseignements personnels que les usagers considèrent comme les plus intimes. Pour garantir la confiance de l'utilisateur dans le système, il faut s'assurer que des moyens soient mis à sa disposition pour lui garantir un certain contrôle sur ses

²⁵⁴ Nous rejoignons sur ce point Richard L'ANGELIER, qui précise: « Par ailleurs, il ne faut pas faire du consentement en matière médicale et sociale, une panacée, dans la mesure où ce consentement est le plus souvent formel, compte tenu de la nature des services rendus et des rapports qui lient un usager avec les professionnels chargés de lui prodiguer des soins ou de lui offrir des services. » L'ANGELIER Richard, Numérisation des dossiers de santé et protection des renseignements personnels: Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes, *Lex Electronica*, vol. 9 été 2004, pp. 2-4 [En ligne] http://www.lex-electronica.org/fr/resumes_complets/97.html (page consultée le 13 septembre 2009)

Le dossier de santé électronique:
le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux

informations, mais également garantir aux patients qu'ils seront informés en cas de violation de conditions d'accès aux dossiers de santé électronique.

Les sanctions en cas de violation de la protection des renseignements personnels sur la santé doivent être à la mesure de la valeur accordée par les usagers à ce type de renseignements. On constate que certaines législations ont mis en place des sanctions dissuasives, ce qui n'est pas le cas du Québec.

Il est également nécessaire de former toutes les personnes qui collectent, utilisent ou divulguent des renseignements personnels de santé aux exigences légales relatives à la protection des renseignements personnels. Pour éviter, notamment les bris de confidentialité, la perte de données et autres événements de ce genre qui amenuisent la confiance que les usagers peuvent avoir à l'égard du système des soins de santé, lorsque celui-ci traite et gère les renseignements personnels de santé des usagers.

Concernant les utilisations secondaires, la meilleure approche consisterait à les interdire, purement et simplement. Cependant, si les législateurs envisagent la possibilité d'utilisation secondaire, qui peut être utile dans le cadre de recherches scientifiques, il faut s'assurer que les usagers consentent expressément à cette finalité, et également que les renseignements personnels soient rendus anonymes selon des normes très strictes.