ÉTUDE SUR L'INFOROUTE DE LA SANTÉ AU QUÉBEC : ENJEUX TECHNIQUES, ÉTHIQUES ET LÉGAUX

DOCUMENT DE RÉFLEXION

COMMISSION D'ACCÈS À L'INFORMATION

Préparé par
Christian Boudreau

OCTOBRE 2001

AVANT-PROPOS

La Commission d'accès à l'information du Québec rend publique une étude qu'elle a effectuée concernant la mise en réseau des dossiers cliniques informatisés en matière de santé. L'objectif poursuivi par la Commission dans la réalisation de cette étude est de contribuer à un débat qu'elle veut public sur les enjeux complexes qui accompagnent la mise en place d'une inforoute de santé.

Cette étude n'a pas la prétention d'être complète ou de traiter de façon définitive l'ensemble des questions sur le sujet, mais de marquer un pas en avant dans une réflexion qui nous interpelle collectivement et individuellement et qui nous conduira à l'élaboration de paramètres nationaux en matière de gestion du dossier clinique informatisé.

La Commission tient à remercier M. Christian Boudreau qui a réalisé cette étude sous la direction de M^{e} Denis Morency, directeur de l'analyse et de l'évaluation, et à souligner les contributions de M^{e} Danielle Parent de la Direction des services juridiques et de M^{me} Sylvie Prigent, analyste en informatique, ainsi que du docteur Jean Ouellet.

TABLE DES MATIÈRES

LISTES DES FIGURES

Page

INTRODUCTION

Les bénéfices cliniques et économiques liés au déploiement d'une inforoute de la santé semblent faire de plus en plus consensus auprès de différents acteurs sociaux et gouvernementaux. Caractérisée par la mise en réseau ou interconnexion de dossiers cliniques informatisés habituellement entreposés dans les lieux de dispensation de soins distincts, l'inforoute vise à améliorer la circulation des renseignements de santé auprès de différents intervenants. Ainsi, elle peut contribuer à éclairer la décision clinique en temps opportun, à favoriser une utilisation appropriée des ressources et à réduire les coûts reliés à la gestion des dossiers.

Besoin de savoir et droit à la vie privée : un fragile équilibre

Un préalable à cette inforoute de la santé est l'informatisation des dossiers cliniques d'établissement et autres organisations de soins et de services de santé. Comme le suggèrent Safran et Goldberg (2000), les nombreux inconvénients associés au dossier patient papier tendent à paver la voie au dossier patient informatisé.

> First, hand-written notes can be illegible. Paper records frequently have missing information or may be unavailable at the time of a patient encounter. In clinics and hospitals, records are unavailable because they have not been returned or are in use in another setting. Paper records can only be in more than one place at the same time if completely photocopied … Over time, paper records costly to maintain, store and retrieved. In a 500-bed hospital, a 7-inch stack of laboratory reports must be filed each day! The cost of simply pulling a chart for a clinic visit and returning that chart for a clinic visit and returning that chart to the file room could exceed US$10 … finding aggregate patient information for clinical research or practice management from a set of paper records is very time consuming. Finally, paper records are not secure[1].

Or, présentement, près de 50 % des établissements de santé au Québec n'ont toujours pas de systèmes cliniques informatisés en laboratoire, en radiologie, en pharmacie et en soins infirmiers[2]. Et quand il y a informatisation des dossiers d'établissement, ces

[1] Safran, C et H. Golberg (2000), Electronic Patient Records and the Impact of the Internet, *International Journal of Medical Informatics,* 60 : 77-83.

[2] François Turenne, allocution prononcée au Salon annuel *Informatique-Santé* de l'AHQ, 22 novembre 2000.

systèmes souvent « ne se parlent pas »; c'est comme s'ils étaient conçus de façon isolée, sans vision d'ensemble, fait remarquer le Vérificateur général.

> Chaque entité – centre local de services communautaires, clinique privée ou urgence - fait cavalier seul en ce qui a trait à la réforme de ses systèmes d'information concernant les patients ambulatoires. Cette situation nuit à l'intégration des activités médicales et ne permet pas de produire en temps opportun une information uniforme, comparable et pertinente. De plus, les systèmes actuels n'assurent pas la circulation de l'information entre les médecins et les lieux de dispensation, ce qui entrave le bon fonctionnement des réseaux de services intégrés[3].

Le déploiement de l'inforoute, c'est-à-dire la mise en réseau des dossiers cliniques informatisés, est vu, souvent avec raison, comme une solution au problème de circulation de l'information dans le secteur de la santé. Cependant, en voulant régler le problème de la circulation des renseignements cliniques, on peut en créer d'autres tout aussi importants. En effet, si les réseaux d'information offrent une infrastructure technologique capable d'améliorer l'efficacité et l'efficience des systèmes de santé, notre soif de connaissances pourrait aussi noyer le professionnel de la santé dans un océan d'information. Regrouper l'information clinique disponible n'est souvent pas suffisante, encore faut-il l'organiser intelligemment de manière à diriger rapidement le professionnel vers les informations pertinentes au regard de la situation particulière de l'usager.

Mais plus inquiétant encore, un déploiement à la hâte d'une inforoute de la santé peut devenir une source de risques qui menacent la vie privée de l'ensemble des Québécoises et Québécois. La circulation de l'information clinique et le droit à la vie privée ne sont pas antinomiques. Cependant, l'équilibre est complexe et fragile quand il s'agit de mettre en œuvre ces deux principes dans le contexte d'une inforoute de la santé. C'est un domaine où l'on ne peut se permettre d'improviser compte tenu de l'importance et de la complexité des enjeux que soulève cette mise en œuvre. C'est aussi un domaine où il n'existe pas de solutions simples, de recettes miracles. Les solutions ou directives proposées devront s'adapter à la réalité des professionnels et des usagers qui les appliqueront. Le défi à relever est de taille, celui de garantir la

[3] Vérificateur général du Québec, Rapport annuel 1999-2000.

confidentialité des renseignements personnels tout en permettant aux intervenants concernés de prendre des décisions cliniques les plus éclairées possibles.

Complexité des enjeux

La circulation des renseignements cliniques informatisés à l'extérieur des établissements et leur protection soulèvent des enjeux qui concernent non seulement la collectivité et son bien-être, mais aussi l'individu dans ses dimensions les plus intimes. Autrement dit, il ne s'agit pas que d'une question d'intérêt public, mais aussi celle d'un droit individuel fondamental, à savoir le respect de la vie privée. Ce n'est pas non plus uniquement l'affaire de l'État et de quelques gestionnaires ou autres experts. Il importe d'en débattre publiquement afin de bien saisir et de gérer de façon éclairée la complexité des enjeux qui nous interpellent individuellement et collectivement. Cela présuppose une volonté de discuter ouvertement des intérêts légitimes et, parfois, divergents des différents agents concernés. La réflexion sera d'autant plus riche qu'elle fera intervenir différents acteurs : citoyens ou groupes de citoyens, État, établissements de santé, associations et ordres de professionnels, groupes communautaires et autres représentants de la population, entreprises privées, etc. En faisant référence à l'informatisation et la mise en réseau des dossiers cliniques, le Collège des médecins soutient que

> [l]a situation actuelle donne l'image de règles multiples à suivre, incomplètes et souvent incomprises, ne formant pas un tout intégré et «compréhensif», mais plutôt un genre de courtepointe. Il y a lieu d'ouvrir un débat sur les véritables besoins de protection des renseignements personnels, et sur les caractéristiques des outils de protection dont on dispose, incluant leurs limites[4].

Le principal objectif poursuivi dans le présent document est d'alimenter de façon constructive une réflexion qui porte sur la circulation et la protection des renseignements personnels dans le cadre du déploiement d'une inforoute de la santé au Québec. Affirmons d'entrée de jeu que la Commission d'accès à l'information n'est pas contre une meilleure circulation des renseignements cliniques à l'extérieur des établissements et autres organisations de soins de santé. L'informatique peut même constituer un puissant outil permettant d'appuyer la décision clinique tout en

protégeant les renseignements cliniques des individus concernés et en préservant leur vie privée. La Commission l'a d'ailleurs signalé dans son avis (1996) sur le projet pilote de cartes santé à microprocesseur mené dans la région de Rimouski. Il n'en demeure pas moins que les outils technologiques, en particulier l'informatique, doivent être considérés comme des moyens et non comme des finalités.

Plan et portée du document

Ce document comprend quatre chapitres. Dans le premier, nous avons analysé sept projets de mise en réseau des dossiers cliniques que nous jugeons représentatifs des mouvements qui sont à la base du déploiement de l'inforoute de la santé au Québec. Dans le deuxième, nous dégageons à la lumière de ces projets des modèles de consentement, des modèles d'entreposage de données et des tendances technologiques émergentes. Nous y traitons aussi d'enjeux qui caractérisent l'avènement d'une inforoute de la santé au Québec, à savoir 1) le décloisonnement des dossiers cliniques, 2) la détention de dossiers cliniques centralisés et réseautés et 3) la création d'un Index Patient National. Le troisième, qui traite du contexte juridique en matière de protection des renseignements personnels au Québec, met en évidence la portée et les limites des règles légales dans le cadre de l'inforoute de la santé. Le quatrième porte sur le consentement, ses principes de validité et son application dans des situations cliniques particulières. Vous trouverez en annexe une description très sommaire des règles relatives à la protection des renseignements personnels aux État-Unis (annexe I) et en Europe (annexe II).

Il convient de préciser la portée du présent document en indiquant que son propos ne porte pas tant sur l'informatisation des dossiers cliniques et de leur accès *à l'intérieur* des organisations de soins de santé que sur la circulation de ces renseignements *à l'extérieur* de ces organisations. Le propos se limite aussi à la situation québécoise et, plus particulièrement, à son système public de santé. Les récents développements de services de santé dans le secteur privé, comme les services en ligne à partir d'Internet ou du téléphone, n'y sont pas abordés. Enfin, il faut comprendre de la nature du document que l'analyse des projets n'en constitue pas un examen de la part de la Commission.

---

[4] Collège des médecins, mémoire déposé au Colloque sur les orientations stratégiques du MSSS,

juin 2000.

1. PROJETS QUÉBÉCOIS

Nous abordons dans ce chapitre divers projets qui reflètent les principales tendances de mise en réseau des dossiers cliniques au Québec. Alors que certains de ces projets sont en phase de conception ou en voie d'implantation (Dossier Patient Partageable, Carte d'Accès Santé et Réseau mère-enfant), d'autres sont déjà en opération (Brome-Missisquoi-Perkins (BMP), SI-PRSA) ou en voie de terminaison (Carte Santé à Laval). Nous avons aussi retenu un projet dont l'expérimentation s'est terminée en mars 1995 (Carte Santé à Rimouski).

1.1 Projet de carte santé à microprocesseur à Rimouski : un dossier patient portable

Description

Dans ce projet d'expérimentation d'une durée de deux ans (1993-1995), l'usage de la carte à microprocesseur visait à rendre disponible à plusieurs intervenants de la santé un dossier de santé minimal, et ce de façon sécurisée. Cette carte se voulait un aide mémoire informatisé que l'usager transportait avec lui et qu'il pouvait présenter quand il consultait un professionnel de la santé. Il s'agissait essentiellement, d'une part, d'un outil de communication entre l'usager et les intervenants de la santé et entre ces derniers et, d'autre part, d'un outil de consentement entre les mains de l'usager. Bien qu'alimentée par des intervenants, la carte santé n'était ni le dossier d'un établissement, ni celui d'un professionnel, mais le dossier de l'usager. Non seulement ce dernier en contrôlait-il les accès et les mises à jour, mais il en était le gardien. Si l'usager perdait sa carte, on lui en émettait une autre, sans le contenu de la précédente. Les professionnels de la santé étaient toujours tenus de remplir leur dossier ou ceux des établissements auxquels ils sont rattachés. La carte santé se superposait donc aux systèmes existants.

> 92 p.100 des omnipraticiens, 52,5 p. 100 des médecins spécialistes, ainsi que la totalité des pharmaciens, des infirmières visées et des ambulanciers ont adhéré au projet [5].

[5] RAMQ (1996), *Évaluation du projet d'expérimentation de la carte santé à microprocesseur. Version abrégée du rapport final* : 18.

Les lieux de dispensation de soins équipés d'un système de cartes santé à microprocesseur étaient le Centre hospitalier régional de Rimouski (CHRR), les cliniques privées de médecins, les pharmacies communautaires, le CLSC de l'Estuaire, le Foyer de Rimouski et les compagnies d'ambulance. 7 248 cartes santé ont été délivrées à des usagers : 4 675 à des personnes de 60 ans et plus, 953 à des nourrissons, 303 à des femmes enceintes et 1 317 à des résidents de St-Fabien. « 73 p. cent des usagers ont utilisé leur carte au moins une fois au cours de l'expérimentation »[6]. Quant aux intervenants de la santé, 257 cartes d'habilitation leur ont été délivrées, dont 156 à des médecins, 57 à des pharmaciens, 34 à des infirmières et 10 à des ambulanciers. Dans le cas des médecins et des pharmaciens, plus d'une carte pouvait leur être délivrée selon le nombre d'endroits où ils travaillaient et qui étaient équipés d'un système de cartes. Par contre, pour le personnel infirmier et le personnel ambulancier, les cartes d'habilitation n'étaient pas attribuées individuellement. Une carte d'habilitation a été remise au responsable de chacune des unités de soins infirmiers dotées d'un système de cartes et à chaque propriétaire de services ambulanciers.

Le contenu de la carte était divisé en zones d'information (identification, urgence, vaccination, médicaments et suivi médical) afin de différencier les accès selon les champs de pratique des intervenants. Le système de cartes santé intégrait aussi trois aides à la décision : un aviseur pharmacothérapeutique, un guide d'immunisation et un module de prévention. La majorité des utilisateurs interrogés (300 usagers, 136 professionnels de la santé et 22 ambulanciers) perçoivent la carte santé comme un outil qui « permet d'améliorer la circulation de l'information clinique, et ce, de façon confidentielle »[7]. La majorité des médecins interrogés considèrent aussi que l'utilisation de l'aviseur pharmacothérapeutique leur a permis de prévenir des complications liées à la médication. Les professionnels de la santé ont néanmoins soulevé certains irritants quant à l'utilisation de la carte santé : « double écriture, lenteur du transfert du système de gestion d'officine vers *Pharmacarte*, prolongation de la durée de consultation, etc. »[8].

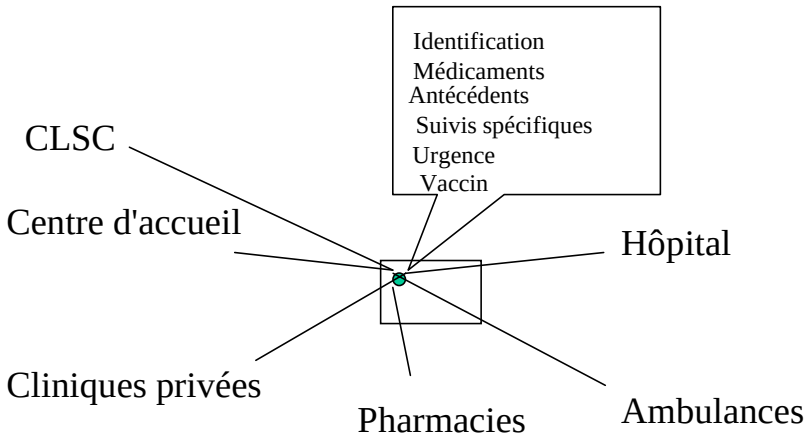
> Si cette expérimentation a démontré l'utilité pour les intervenants de partager l'information, [elle a aussi] indiqué que les données inscrites sur la carte de

[6] *Ibid.* : 19.
[7] *Idem.*
[8] *Ibid*. : 26.

l'usager devaient être complétées par d'autres données conservées à distance[9].

Figure 1

Architecture Carte Santé Rimouski



Alimentation, accès et consentement

L 'accès au contenu de la carte de l'usager nécessitait l'utilisation d'une carte d'habilitation détenue par l'intervenant. En décidant de présenter ou non sa carte santé à l'intervenant, l'usager pouvait contrôler la communication de son contenu à des tiers. L'usager avait aussi le pouvoir de refuser que certains renseignements y soient inscrits ou de rendre non visible pour les intervenants une donnée déjà inscrite sur sa carte. Enfin, l'usager pouvait accéder au contenu de sa carte lorsqu'il consultait un intervenant de la santé ou s'il se rendait au Bureau de la carte santé. L'accès au contenu de la carte se faisait soit par une visualisation à l'écran, soit par une impression papier. Or,

> [l]es médecins rencontrés en entrevue affirment que peu d'usagers se prévalent de leurs droits de consulter l'information à l'écran, de la modifier et d'obtenir une copie imprimée du contenu de la carte. Seulement quatre demandes de consultation, deux demandes d'imprimés et une demande de modification ont été adressées directement au Bureau de la carte santé[10].

---

[9] Rémy Trudel, mémoire déposé au Conseil des Ministres, intitulé *L'implantation de la Carte d'accès Santé à microprocesseur et la contribution de la RAMQ à la modernisation du système de Santé et des Services sociaux*. le 2 avril 2001 : 1.

[10] RAMQ (1996), *op. cit*. : 103.

À cet égard,

> Des usagers ont signalé [en entrevue] que le fait de regarder ce qui est inscrit sur la carte, au moment de la consultation, peut être perçu comme un manque de confiance envers son médecin[11].

Enfin, soulignons que les applications qui géraient la mise à jour des cartes santé permettaient de filtrer l'inscription de certains renseignements socialement sensibles, en particulier ceux relatifs aux problèmes psychiatriques ou psychologiques.

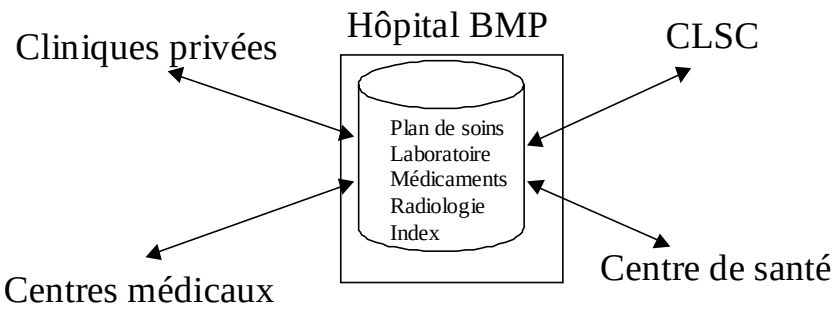
1.2 Inforoute Santé BMP[12] : un dossier d'établissement accessible régionalement

Description

Le système déployé dans le cadre de cette inforoute, qui est toujours en opération, vise à rendre accessibles en tout temps des données du dossier hospitalier de l'hôpital BMP à des professionnels de la santé qui sont rattachés à un CLSC, à des cliniques privées ou à des CHSLD. Plus précisément, les utilisateurs du système peuvent utiliser un logiciel (Médiplan) permettant d'accéder à des informations relatives à l'épisode de soins d'un usager, de mettre à jour le dossier pharmacologique de l'hôpital et l'index bénéficiaires, de prescrire des examens radiologiques et des examens de laboratoire et de recevoir les résultats de ces examens. Autrement dit, il s'agit d'une mise en réseau d'un dossier hospitalier afin de suivre l'évolution de l'état de santé d'un usager aussi bien à l'intérieur de l'hôpital qu'à l'extérieur de celui-ci.

Figure 2

Architecture de l'Inforoute Santé BMP



[11] *Idem.*

[12] Pour ce système, nous disposons d'information qui ne dépasse pas l'année 1997.

Alimentation, accès et consentement

Dans ce système, l'usager autorise par écrit tous les utilisateurs du réseau à accéder à distance à des éléments du dossier de l'hôpital BMP selon des droits d'accès différenciés. Bien que révocable en tout temps, cette autorisation de consultation à distance ne précisait aucune durée en 1997. Pour accéder par le réseau aux dossiers informatisés de l'hôpital BMP, les professionnels de la santé doivent inscrire leur code d'utilisateur et leur mot de passe[13]. L'accès à l'index bénéficiaires (ou index patients) ne requiert pas l'autorisation de l'usager, tout comme l'accès par les intervenants de l'urgence au dossier informatisé[14]. Le système permet une journalisation des mises à jour et des visualisations du dossier. En ce qui concerne les utilisateurs de cette inforoute régionale, 54 % sont des infirmières contre 46 % des secrétaires[15].

1.3 Dossier patient partageable : un dossier régional

Description

Le Dossier Patient Partageable est davantage un concept qu'un projet. Tel que l'envisage la SOGIQUE, le Dossier Patient Partageable vise à rendre accessibles des données cliniques déjà saisies et entreposées dans différents dossiers d'établissements et autres organisations de santé. Il s'agit d'une nouvelle banque de données qui s'ajoute aux dossiers existants, d'« une fenêtre sur des données existantes relatives à un patient sur des systèmes jusqu'à maintenant fermés »[16]. Les responsables du projet Dossier Patient Partageable partent de la prémisse

> qu'une application informatique de Dossier patient électronique dans laquelle les utilisateurs seraient initialement obligés de saisir au complet les données présentes, n'aurait aucune chance de s'implanter avec succès. L'orientation

[13] En août 1997, le mot de passe était commun pour les intervenants de l'urgence, du bloc opératoire et de la clinique Nesbitt.
[14] En 1997, les responsables du réseau s'étaient engagés à faire en sorte « qu'à chaque fois que le *bouton d'urgence* sera utilisé, une journalisation sera effectuée » (Bernard Dionne, note de service du 17 juillet 1997)
[15] Quant à l'utilisation du système à l'intérieur de l'hôpital BMP, 75 % des utilisateurs sont des infirmières, 6,9 % des secrétaires et 1,4 % des médecins.
[16] SOGIQUE, *Rapport synthèse de l'analyse préliminaire du projet dossier patient partageable,* présenté par Réginald Blanchard au colloque de l'AHQ le 23 novembre 2000: 8

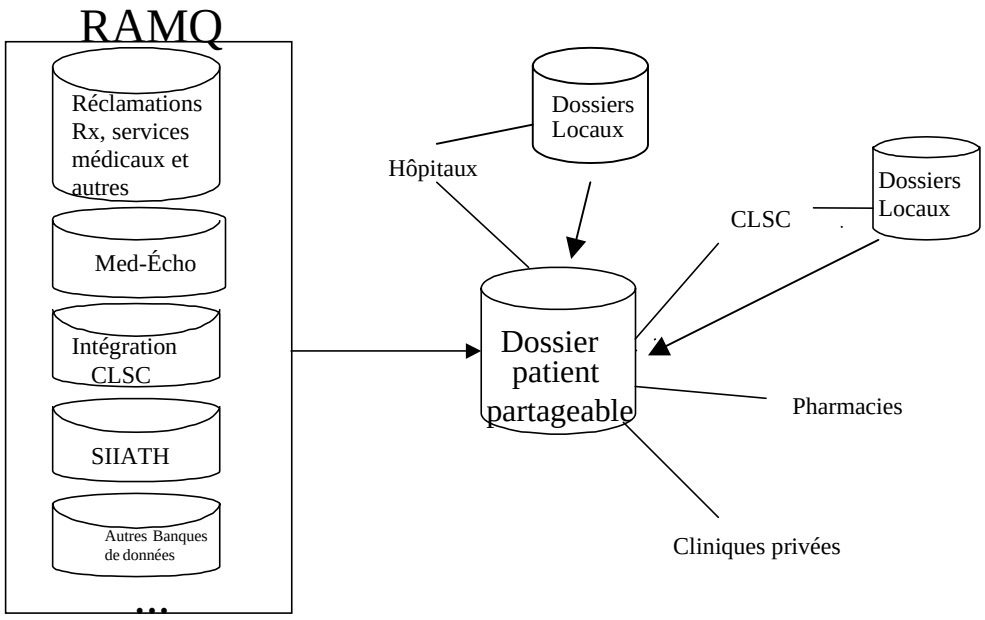
> de départ consiste donc à exploiter des dépôts de données déjà existants ou à venir à la RAMQ et dans les établissements de santé … Les principaux dépôts de données à être accessibles dans la première étape du projet sont ceux de la RAMQ (visites extraites des données du système de facturation, données de séjour hospitalier provenant du système Med-Écho), ceux des pharmacies privées et les dépôts de données des résultats d'analyses de laboratoire et d'examens de radiologie[17].

L'utilisation d'un identifiant unique est essentielle au déploiement du Dossier Patient Partageable, soutiennent les responsables du projet à la SOGIQUE, afin d'établir l'interconnexion entre ce dossier et les systèmes existants.

> L'application DPP … pourra présenter les informations contenues dans d'autres dépôts spécialisés si l'identifiant unique provincial était utilisé par ces autres applications. Ces données deviennent, dans ce cas, des extensions du DPP. On peut, à titre d'exemple, parler de dépôts de données d'images radiologiques, des profils de soins fournis par l'application «intégration CLSC», etc[18].

Figure 3

Architecture du Dossier Patient Partageable



[17] *Ibid.* : 7.
[18] *Ibid.* : 8.

Alimentation, accès et consentement

Le consentement au moment de la visualisation ou de la mise à jour du Dossier Patient Partageable a été analysée par un groupe de travail mandaté par la SOGIQUE. Ce groupe a proposé un système de consentement basé sur un formulaire électronique dans lequel l'usager aurait eu à préciser les organisations de services qui pouvaient, d'une part, alimenter leur dossier patient partageable et, d'autre part, le visualiser. Or, selon les responsables du projet Dossier Patient Partageable, une telle solution « serait coûteuse et très complexe à réaliser »[19]. Ils recommandent plutôt l'adoption d'un modèle de consentement simplifié qui s'inspire, entre autres, du projet CRUSE-Omnimed dans l'Estrie et de l'inforoute BMP[20]. Ces responsables mettent de l'avant l'idée que les données doivent être accessibles en présence ou en l'absence de l'usager une fois que ce dernier a exprimé son consentement, que ce soit « pour préparer à l'avance la cueillette et l'analyse des données antérieures du patient ou pour poursuivre entre deux rencontres l'analyse et la rédaction de notes au dossier »[21]. Ils soutiennent qu'il serait lourd et non souhaitable d'offrir un Dossier Patient Partageable dont l'accès exigerait que l'usager présente une carte à microprocesseur ou qu'il soumette un NIP,

> en raison notamment des très grands risques reliés à l'oubli du mot de passe reliée à la carte, à l'oubli de la carte elle-même par le patient ou la perte ou altération de cette dernière. Ces risques ont été mentionnés à plusieurs reprises en particulier pour les clientèles d'enfants, de personnes âgées et de personnes peu scolarisées[22].

1.4 Système d'information de la programmation régionale des services ambulatoires de Laval (SI-PRSA) : un dossier épisode de soins régional

Description

Ce projet en opération, dont le déploiement a commencé en août 1998, met en place un système d'information qui supporte les échanges de données cliniques entre des professionnels de la santé engagés dans la prestation de services dans le cadre de différents programmes. Ce projet vise, entre autres, à diminuer la durée d'hospitalisation

[19] *Ibid.* : 5.
[20] *Idem*.
[21] *Ibid.* : 7.
[22] *Ibid.* : 6.

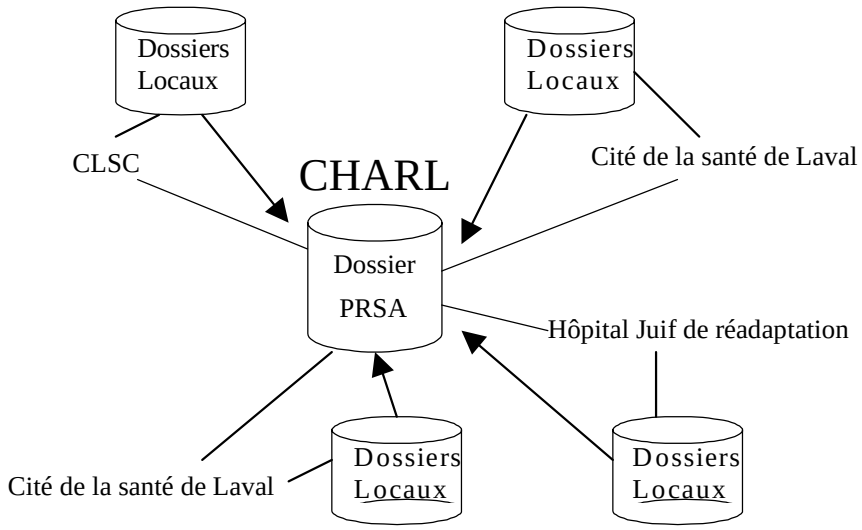
en substituant à des activités hospitalières conventionnelles des activités ambulatoires. L'épisode de soins est central à ce projet. C'est autour de cet épisode que s'articule le plan de soins.

> L'épisode de soins … se caractérise par une intensité de services pour une durée définie dans le temps selon une approche réseau qui garantit la continuité des services et l'implication possible de plusieurs dispensateurs de services[23].

Il exige souvent des soins spécialisés traditionnellement regroupés dans un centre hospitalier. Il peut couvrir la préhospitalisation, l'hospitalisation et la posthospitalisation. Autrement dit, l'épisode de soins suppose l'intervention de plusieurs intervenants de la santé qui doivent s'échanger de l'information à l'intérieur d'un même continuum de soins et de services. Dans le SI-PRSA, le dossier clinique informatisé, qui est crée au début d'un épisode de soins, n'est pas un dossier d'établissement, mais un dossier interétablissement accessible par différentes équipes soignantes le temps que dure l'épisode. Une fois l'épisode terminé, les données du SI-PRSA cessent d'être accessibles aux établissements dispensateurs. Le Centre hospitalier ambulatoire régional de Laval (CHARL) est le fiduciaire et gardien des données cliniques du SI-PRSA.

Figure 4

Architecture SI-PRSA



[23] Régie régionale de la santé et des services sociaux de Laval, Document de positionnement de la sécurité du SI-PRSA, Projet Vitrine PRSA – Carte santé, 13 mars 2001.

Alimentation, accès et consentement

Toute alimentation ou accès au SI-PRSA requiert obligatoirement l'utilisation de la carte de l'intervenant aussi bien sur le plan clinique que sur le plan clérical et administratif[24]. Après avoir inséré leur carte dans un lecteur, les intervenants doivent composer leur NIP. Ceux-ci ne peuvent accéder qu'aux données cliniques des usagers du SI-PRSA qu'ils prennent en charge. Au moment de l'inscription de l'usager au SI-PRSA, un intervenant de la santé habilité ouvre un nouveau dossier. L'usager signe alors un formulaire de consentement autorisant des intervenants de la santé de différents lieux de dispensation de soins à se communiquer des renseignements le concernant et à les mettre à jour. À la fin de l'épisode de soins, le SI-PRSA archive le dossier et cesse de le rendre disponible dans les autres sites. Aucune mise à jour ne peut être effectuée après que le congé ait pris effet. C'est la date du congé qui conditionne la fermeture de l'épisode de soins. Toute communication des données du SI-PRSA après le congé de l'usager requiert l'autorisation de CHARL. Tous les utilisateurs du SI-PRSA peuvent visualiser et mettre à jour les données d'identification de l'usager (Index patient) sans le consentement de ce dernier. Les données du SI-PRSA servent aussi à alimenter des tableaux de bord régionaux. Cependant, le responsable de ces tableaux n'a accès qu'à des données dépersonnalisées.

1.5 Projet Carte santé à Laval : un dossier patient centralisé

Description

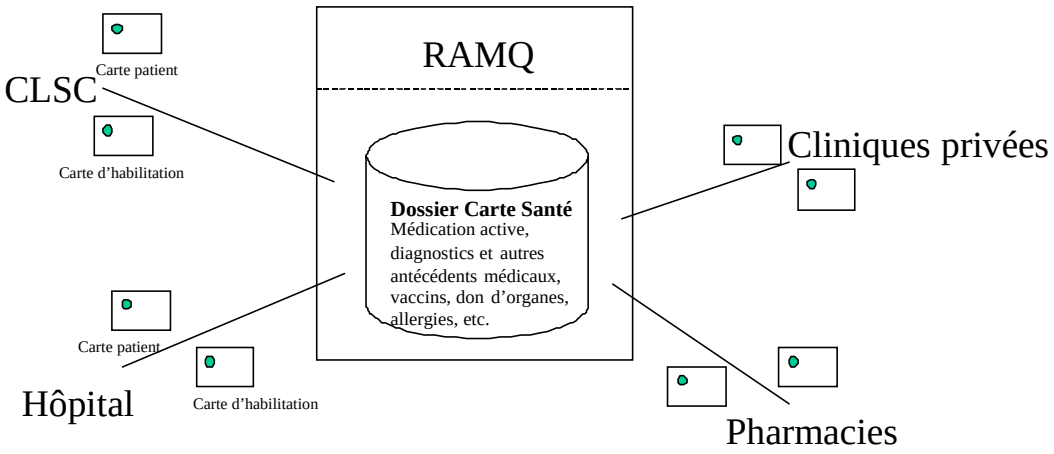
Le projet Carte santé à Laval, dont le déploiement a commencé en septembre 1999, vise à tester les principaux mécanismes d'un système de carte santé à microprocesseur déployé dans un contexte de télécommunication et de centralisation des renseignements cliniques. En plus d'être un dossier portable, la carte santé à microprocesseur est devenue dans ce projet une clé d'accès à un dossier clinique entreposé à la Régie de l'assurance maladie du Québec (RAMQ), nommé Dossier Carte Santé. Il vise plus particulièrement à tester la mécanique du consentement de l'usager quant à l'accès par des tiers à ce dossier ainsi que le transport et l'entreposage

[24] Dans la mesure où la carte à microprocesseur de l'intervenant est une composante technologique introduite lors de l'implantation du projet Carte santé à Laval (voir section 1.5), celle-ci sera-t-elle toujours exigée lorsque que ce projet se terminera?

sécurisés des renseignements qu'il contient. En date du 1er mai 2001, 1 678 cartes santé étaient émises à des usagers. « De ce nombre, seulement 290 cartes ont été activées, c'est-à-dire que seulement 290 patients ont accepté de choisir un numéro d'identification personnel (NIP) afin d'utiliser leur carte ». Quant aux intervenants de la santé, 908 cartes d'habilitation leur ont été distribuées.

Figure 5

Architecture de la Carte Santé à Laval



Alimentation, accès et consentement

Les règles d'alimentation, de communication et de consentement recoupent en grande partie celles mises de l'avant dans les projets de Carte Santé à Rimouski (voir la section 2.1) et de Carte d'Accès Santé (voir la section 2.7). En effet, le consentement explicite et ponctuel de l'usager est requis pour que l'intervenant de la santé mette à jour ou visualise le Dossier Carte Santé. L'intervenant doit au préalable s'habiliter au système en insérant sa carte dans un lecteur approprié et en tapant son NIP. Il doit ensuite insérer la carte de l'usager dans le lecteur. L'usager peut aussi entrer un NIP pour s'authentifier. Comme dans les autres projets, l'accès au contenu clinique est différencié selon les champs et lieux de pratique. Le système enregistre dans un journal les accès au Dossier Carte Santé ainsi que ses mises à jour. Les données qui circulent sur le réseau sont, quant à elles, chiffrées. Contrairement au projet de Carte Santé à Rimouski, le présent système ne permet pas d'apporter des corrections dans le

Dossier Carte Santé : « l'alimentation de toute donnée dans le DCS est définitive et toute information ne peut n'y être corrigée ou détruite »[25]. L'usager peut se retirer à tout moment du projet et, donc, du système de carte santé; l'alimentation du Dossier Carte Santé cesse alors. Les intervenants de la santé peuvent obtenir la liste des noms de leurs patients qui participent au projet et leur adresse tandis que la RAMQ n'y a pas accès.

1.6 Projet Réseau mère-enfant de Sainte-Justine : un dossier régional centralisé

Description

Ce projet en phase de conception vise à « assurer un continuum de soins intégrés par le biais des services offerts par l'équipe de l'Hôpital Sainte-Justine et par les centres hospitaliers régionaux et leur réseau de 1ère ligne »[26]. Plus précisément, il vise à

> améliorer l'accessibilité à l'information clinique pertinente afin de 1) mieux articuler la continuité de soins entre les intervenants, 2) offrir aux intervenants la disponibilité permanente des données cliniques pertinentes au suivi du patient quel que soit leur lieu de conservation, 3) offrir aux intervenants autorisés une porte d'accès unique et conviviale à l'information et 4) réduire les reprises inutiles de tests et d'examens [27].

Ce système permettra, dans un premier temps, de regrouper sur un même serveur des éléments de dossiers de santé que l'on retrouve dans trois hôpitaux (Hôpital Sainte-Justine, Cité de la santé de Laval et Hôpital Saint-Eustache) et dans des cliniques pédiatriques. Les dossiers locaux dans les établissements et les cliniques demeurent autonomes quant à leur mise à jour. L'alimentation de ce Dossier Patient Partageable, entreposé dans un serveur HDN, se ferait de façon automatique, dès que le professionnel inscrirait de l'information dans les dossiers locaux de son établissement ou de sa clinique. Autrement dit, aucune saisie ne se ferait directement dans le Dossier Patient Réseau, celui-ci pompant son information des dossiers existants. Ainsi, le déploiement de ce système dépend du degré d'informatisation des systèmes d'information dans les établissements de santé et les cliniques du fait qu'il s'en alimente. Il dépend aussi de l'utilisation d'un identifiant unique permettant de regrouper

---

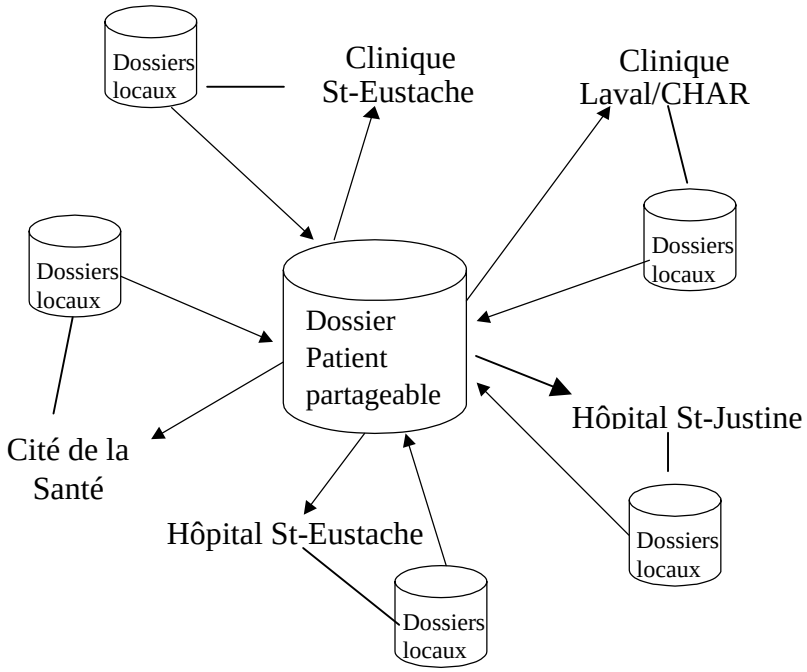
[25] RAMQ, *Procédures d'accès au système de carte santé à microprocesseur. Projet Vitrine PRSA-Carte Santé – Volet Pharmacie.*

[26] Extrait de la présentation du Dr Lucie Poitras fait le 29 mars 2001 au MSSS.

les renseignements des différents dossiers et de constituer ce Dossier Patient Partageable. Les renseignements qui seront versés dans ce dossier à partir des systèmes existants pourront être des données démographiques, la date d'hospitalisation, les diagnostics d'admission, les sommaires d'interventions, les protocoles opératoires, les résultats d'analyse, les rapports de pathologie, les rapports d'examens de laboratoire et les images radiologiques.

Figure 6

Architecture Réseau mère-enfant



Alimentation, accès et consentement

Nous disposons de peu de renseignements sur les mécanismes d'accès au dossier clinique du présent projet, plusieurs paramètres n'ayant pas encore été fixés. Les responsables du projet semblent soutenir que le consentement de l'usager n'interviendrait pas au moment de l'alimentation de ce Dossier Patient Partageable. L'alimentation se ferait automatiquement, dès que le professionnel inscrirait de l'information dans les dossiers locaux de son établissement ou de sa clinique. La nature des renseignements cliniques qui alimenteraient ce dossier serait

---

[27] *Idem*.

prédéterminée. Quant au consentement au moment de la visualisation de ce Dossier Patient Partageable, les règles ne sont pas encore précisées.

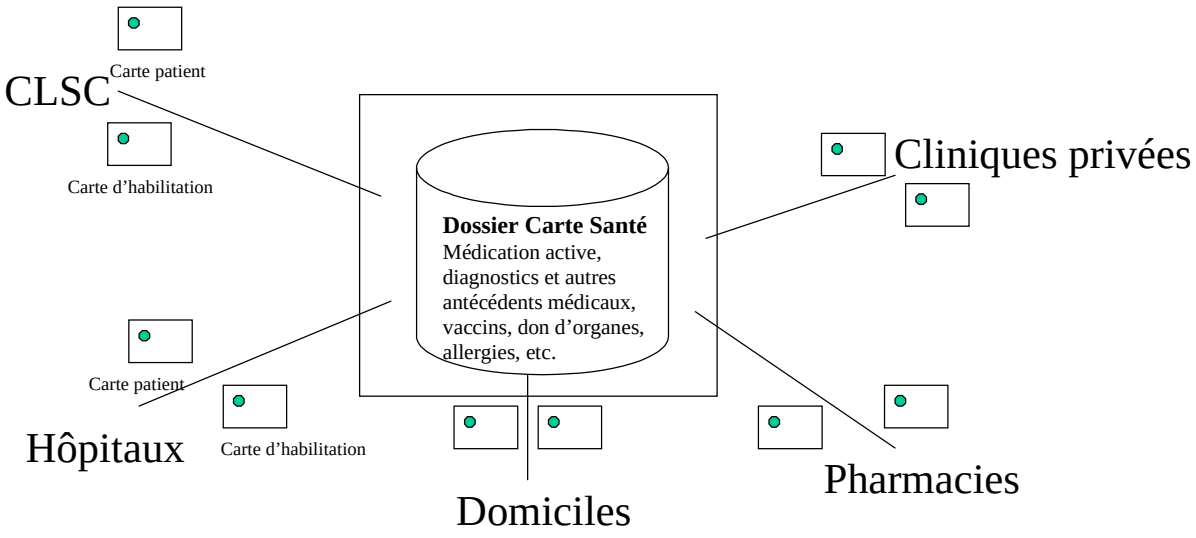
1.7 Projet Carte d'Accès Santé : un dossier patient provincial centralisé

Description

Cet autre projet en phase de conception poursuit trois grandes finalités : 1) la constitution d'un sommaire électronique de données de santé sur l'usager (finalité clinique), 2) la création d'un Index Patient National (finalité clinico-administrative) et 3) l'implantation d'un système de vérification en temps réel de l'admissibilité des assurés et de la facturation des professionnels (finalité administrative). Dans le cas du sommaire électronique, les données seront conservées à la RAMQ dans une banque, appelée ici aussi Dossier Carte Santé, accessible au moyen du réseau de télécommunication sociosanitaire (RTSS). À l'instar du projet Carte Santé à Rimouski et du projet Carte Santé à Laval, l'accès aux données cliniques requerra l'utilisation de la carte de l'usager et de la carte du professionnel. Dans un premier temps, les renseignements qui pourront y être inscrits seront la médication active, les vaccins reçus, certains diagnostics et autres antécédents médicaux.

Figure 7

Architecture du Dossier Carte Santé

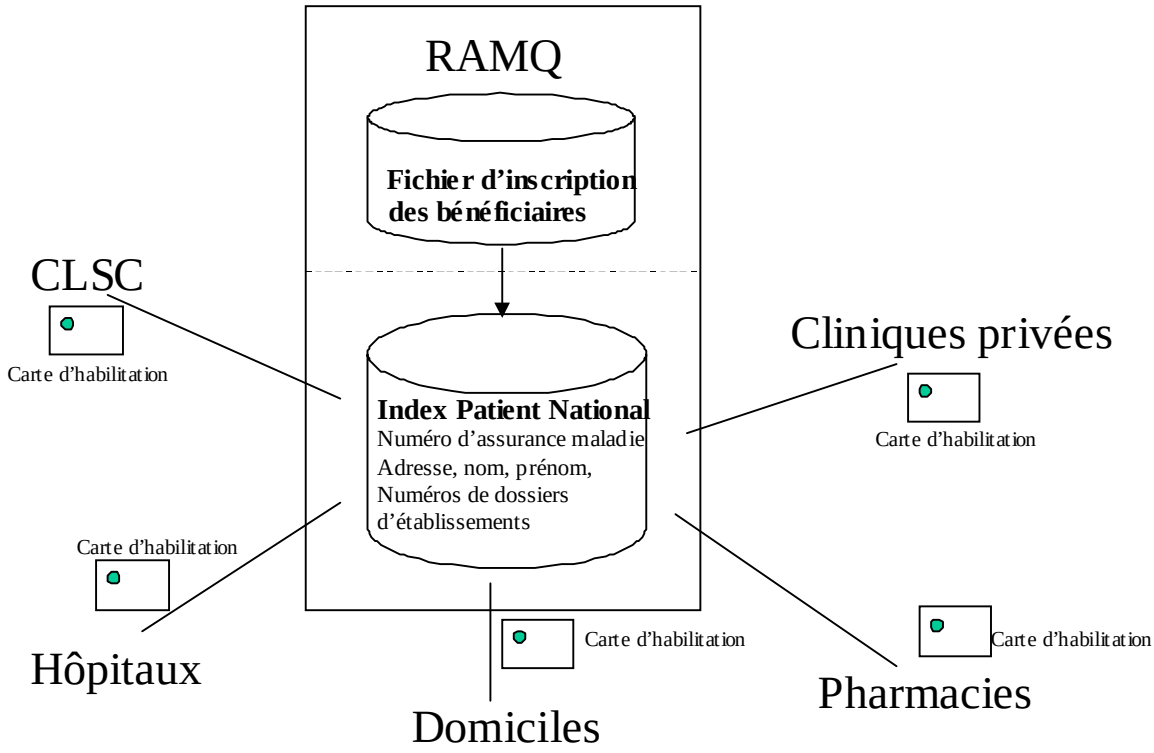


En ce qui concerne le volet clinico-administratif du présent projet, la RAMQ envisage de mettre en place un Index Patient National accessible en tout temps, sans le consentement de l'usager, à partir de tous les établissements et autres organisations de soins au Québec. Avec cet index, les établissements de santé n'auront plus à émettre de carte d'hôpital. L'Index Patient National permettra d'identifier électroniquement l'usager dans tout le système de santé. Cet index s'articulera autour d'un identifiant unique à l'échelle du Québec, soit le numéro d'assurance maladie, ainsi que de données d'identification que gère déjà la RAMQ à partir de son Fichier d'inscription des bénéficiaires, communément appelé le FIB.

> Ainsi, le personnel d'un établissement ou d'un cabinet privé qui désire obtenir l'identifiant ainsi que les données d'identification d'une personne [pourra] le faire en lien direct avec la Régie et ce, sans la présence de la personne concernée. Cet accès est nécessaire dans diverses circonstances comme, par exemple, ouvrir un nouveau dossier, classer un document dans son dossier existant ou préparer une correspondance … Les données complémentaires comme le numéro de dossier de l'établissement … sont mises à jour par les organisations de services[28].

Figure 8

Architecture Index Patient National



[28] *Ibid.* : 9.

Quant au volet administratif du projet Carte d'Accès Santé, il vise 1) à vérifier en direct l'admissibilité de l'usager et la couverture des services assurés, 2) à produire un relevé des services reçus qui sera remis à l'usager afin de le sensibiliser sur les coûts des services consommés et 3) à resserrer les vérifications relatives à la rémunération des professionnels.

En somme, la Carte d'Accès Santé deviendrait la clé unique d'accès au système de santé québécois ainsi qu'aux régimes publics d'assurance santé. Cette carte contiendra, dans son microprocesseur, un ensemble de renseignements comme l'identification, les données concernant le don d'organes et certaines données cliniques. Ainsi, elle permettra au système d'opérer de façon autonome par rapport au réseau, c'est-à-dire en mode déconnecté. Par exemple, la carte de l'usager contiendra des renseignements d'identification sur son titulaire, reproduits aussi dans l'Index Patient National, afin de faciliter une utilisation administrative en mode déconnecté dans les différents lieux de dispensation de soins.

Alimentation, accès et consentement

Comme dans le cas des deux précédents projets de Carte Santé, le présent projet permettra à l'usager de consentir quant à l'alimentation du Dossier Carte Santé et à sa communication à des tiers. L'usager aura aussi les droits suivants vis-à-vis de ce dossier[29]:

- connaître les intervenants qui accéderont à son Dossier Carte Santé, à quel moment et quelle information sera consultée ou mise à jour;
- consulter son contenu et en obtenir une copie;
- demander à l'intervenant de la santé qui aura inscrit des renseignements d'y apporter des rectifications lorsque ceux-ci seront jugés inexacts, incorrects ou équivoques et dans la mesure où les corrections demandées viseront des renseignements objectifs et vérifiables;
- demander la destruction de tout renseignement qu'il ne désirera plus voir inscrit à son Dossier Carte Santé.

Il s'agira, précise-t-on, d'un aide mémoire facultatif. Comme le Dossier Patient Portable, le Dossier Carte Santé se superposera aux dossiers existants à la différence que l'usager en contrôlera non seulement l'accès par des tiers, mais aussi son alimentation.

Contrairement à la constitution du Dossier Carte Santé, l'inscription par la RAMQ de renseignements personnels d'identification dans l'Index Patient National ne nécessitera pas le consentement de l'usager. Il en serait de même pour la consultation et la mise à jour de cet index par les organisations de dispensation de soins.

Afin d'assurer l'intégrité et la disponibilité des données en cas de bris de système ou de pertes de cartes, la RAMQ envisage effectuer des copies de sauvegarde des renseignements contenus dans les différentes banques qui alimentent le présent système, dont le Dossier Carte Santé, l'Index Patient National et le contenu des cartes santé en circulation[30]. Cependant, on précise dans le mémoire que

> [e]n aucun temps, en tant qu'administrateur du système, la Régie n'a accès au contenu du DSC. L'information contenue au dépôt de données DCS est traitée par un mécanisme qui en rend l'interprétation impossible sans le consentement de l'usager. Ainsi, les renseignements d'un dossier sont chiffrés avec une clé de chiffrement propre à chacun des usagers[31].

Le ministre souligne que les renseignements personnels portés au Dossier Carte Santé de l'usager ne pourront pas être utilisés pour des finalités autres que cliniques et que, pour ce faire, il faudra prévoir un cadre juridique interdisant l'accès aux assureurs, même public, ou aux employeurs[32]. Enfin, le ministre confère à la RAMQ les pouvoirs d'une autorité de certification qui délivrera, dans le cadre d'une infrastructure à clés publiques,

> à chaque intervenant une carte d'habilitation à microprocesseur renfermant un certificat d'identité accessible par un NIP connu seulement de l'intervenant ... La délivrance des cartes et des certificats est de la responsabilité directe de la Régie[33].

---

[29] Voir, notamment, l'*Annexe I : Protection des renseignements personnels du mémoire*, déposé par le ministre Rémy Trudel au Conseil des ministres (2001), *op. cit.*

[30] Clés, certificats, données d'identification et renseignements de santé.

[31] Annexe I, *op. cit.*

[32] Voir en particulier la section 10 de l'Annexe I. Les garanties de sécurité, *op. cit.*

[33] *Idem.*

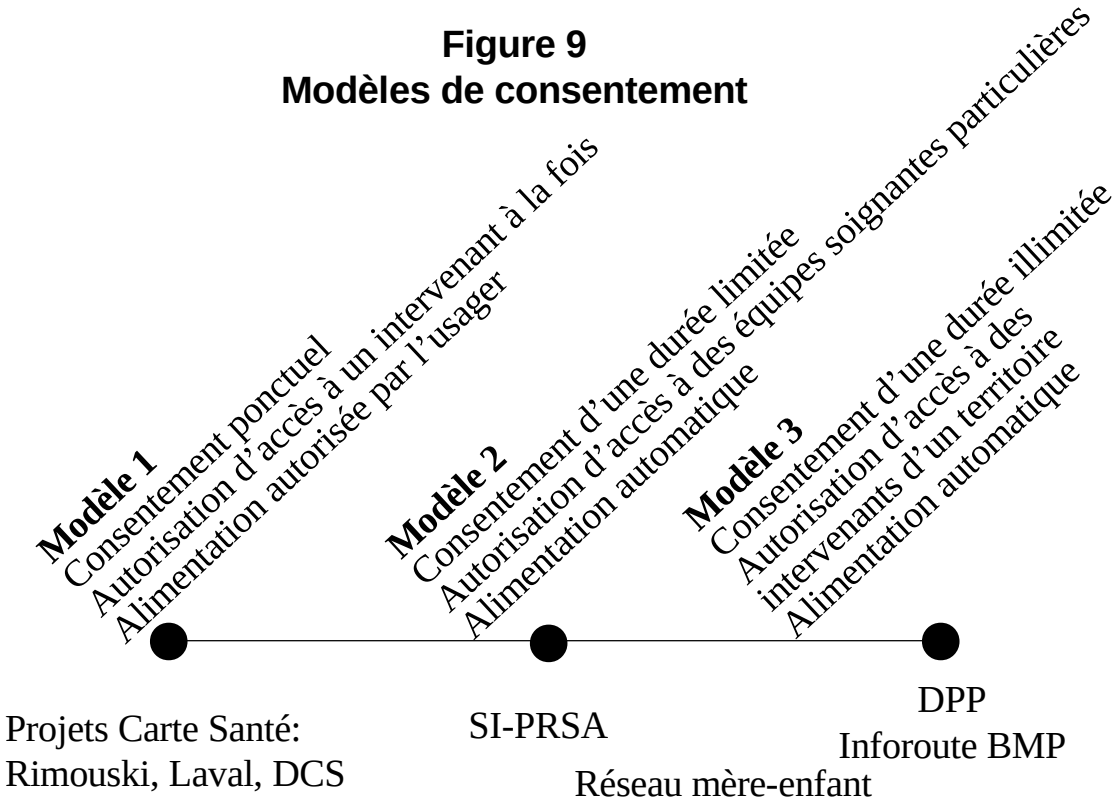
2. MODÈLES DE CONSENTEMENT, MODÈLES D'ENTREPOSAGE ET TENDANCES

À la lumière des précédents projets québécois, on peut dégager des modèles de consentement et des modèles d'entreposage à partir desquels semblent se développer l'inforoute de la santé au Québec. On observe aussi l'émergence de tendances sur lesquelles il convient de s'attarder : 1) la création de grands réseaux de télécommunication de renseignements de santé, 2) la constitution de dossiers cliniques centralisés et 3) la création d'un Index Patient à l'échelle provinciale.

2.1 Modèles de consentement

Du point de vue de la communication à des tiers de renseignements de santé personnels dans un contexte réseauté, les projets québécois montrent que le consentement peut être 1) ponctuel, en général valable le temps que dure la consultation du professionnel, 2) d'une durée limitée, par exemple le temps que dure l'épisode de soins ou 3) d'une durée indéterminée, tant et aussi longtemps que l'autorisation d'accès n'est pas révoquée par l'usager. Nous constatons aussi que l'usager peut autoriser l'accès à ses renseignements de santé 1) à un intervenant à la fois, 2) à des équipes soignantes particulières ou 3) à des intervenants d'une territoire donné. Mis à part les projets de carte santé à microprocesseur, le consentement n'est pas sollicité lors de l'alimentation des dossiers cliniques mis en réseau. La logique hospitalière de tenue de dossier semble être alors prédominante, l'alimentation se faisant à partir d'une réplication automatisée des dossiers existants. À la lumière des projets québécois étudiés, on peut dégager trois modèles de consentement dans l'actuel déploiement de l'inforoute (voir Figure 9).

Figure 9
Modèles de consentement



C'est dans le modèle 3 que l'usager exerce le consentement le plus étendu et le plus flou à la fois sur le plan spatial et sur le plan temporel. Pour l'usager, cela revient à donner accès à des intervenants de la santé d'un territoire donné pour une période indéterminée. Quant au consentement ponctuel et ciblé du modèle 1, bien adapté dans certaines situations comme les problèmes de santé ponctuels, il peut paraître plus difficile d'application dans d'autres circonstances, comme en situation d'urgence ou lors d'un épisode de soins. Pour ce qui est du modèle 2, s'il semble bien adapté aux soins hospitaliers et, plus globalement, à un épisode de soins, il semble moins bien approprié pour faire face aux situations d'urgence ou aux problèmes de santé ponctuels (nous y reviendrons au chapitre 4).

2.2 Modèles d'entreposage des données cliniques

Quatre grands modèles d'entreposage des données cliniques émergent des premières tentatives de déploiement de l'inforoute de la santé au Québec. Nous regroupons ces modèles sous l'informatisation et la mise en réseaux des dossiers suivants :

- dossiers portables;
- dossiers locaux;
- dossiers centralisés sur une base régionale;
- dossiers centralisés sur une base provinciale.

Dossiers électroniques portables

Le projet Carte Santé à Rimouski, qui repose sur la technologie des cartes à microprocesseur en tant que dossiers électroniques portables, illustre bien ce premier modèle d'entreposage de données. Dans ce projet, l'usager transportait avec lui une carte contenant un dossier de santé minimal ainsi que des données d'identification, des clés et des mots de passe. L'évaluation de ce projet (RAMQ 1996) a mis en évidence le besoin d'accéder à des informations dont le volume dépasse largement l'espace disponible sur la carte, en particulier les examens de laboratoire et autres examens diagnostiques. Les récents développements et projets dans le domaine des cartes à microprocesseur, à tout le moins au Québec, s'orientent vers l'utilisation d'une carte donnant accès à des réseaux d'information et à des services assurés. Cela ne signifie pas pour autant la fin de la carte à microprocesseur comme dossier portable. Même dans un contexte d'inforoute, cette carte continuera à contenir de l'information, dont des clés, des mots de passe, des profils d'accès, des certificats, des renseignements d'identification personnels, des numéros de dossiers de santé et des renseignements de santé de base. La carte en tant que dossier électronique portable est d'ailleurs présente dans le projet de Carte Santé à Laval ainsi que dans celui de la Carte d'Accès Santé.

Dossiers électroniques locaux

L'interrogation à distance des dossiers électroniques locaux est certainement un des modèles de mise en réseau les plus courants. Il consiste généralement en un réseautage de dossiers d'établissement existants. Les renseignements de santé que les établissements rendent disponibles peuvent avoir été collectés au moment d'une hospitalisation, d'une chirurgie d'un jour, d'une consultation médicale ou d'un examen diagnostique (laboratoire, imagerie, etc.). Le projet de l'inforoute BMP témoigne de ce modèle de dossiers locaux, comme bien d'autres projets d'ailleurs : CUSE, l'Hôtel-Dieu

de Lévis, le centre hospitalier St-Eustache, etc. La mise en réseau des dossiers locaux est évidemment fonction du degré d'informatisation des établissements et autres organisations qui dispensent des soins de santé. Or, si les systèmes de facturation sont informatisés et réseautés dans la majorité des cas[34], les systèmes de dossiers cliniques dans ces mêmes organisations fonctionnent souvent sur support papier. L'informatisation des réseaux de communication internes aux établissements de santé est d'ailleurs une des priorités du MSSS[35]. Pour l'instant, seules les pharmacies communautaires sont équipées en majorité de dossiers cliniques entièrement informatisés[36].

Dossiers électroniques centralisés sur une base régionale

Selon ce modèle d'entreposage, les utilisateurs du système interrogent un nouveau dossier qui peut être alimenté par différentes organisations de soins : hôpitaux, CLSC, cliniques privées, pharmacies, etc. Il s'agit d'accéder non plus directement, comme dans le précédent modèle, aux différents dossiers locaux, mais à un dossier qui centralise des éléments de dossiers locaux d'une même région. Le Dossier Patient Partageable, tel que conçu par des responsables de la SOGIQUE, le Réseau mère-enfant et le SI-PRSA s'inscrivent dans cette logique de développement des dossiers informatisés. Ce modèle d'entreposage décloisonne les frontières traditionnelles des dossiers basées sur le lieu de dispensation de soins. L'information que les professionnels inscrivent aux dossiers locaux de l'établissement ou autres organisations de soins est répliquée automatiquement dans une banque de données que pourront visualiser les professionnels de la santé. Autrement dit, plutôt que d'interroger les dossiers locaux existants, l'utilisateur du système accède à une banque centralisée sur une base régionale. La constitution de cette banque est fonction, elle aussi, du degré d'informatisation des organisations qui dispensent des soins.

---

[34] Sur les 105 millions de demandes de paiement traitées par la RAMQ, en 1998-1999, environ 100 millions (95 %) ont été reçues sous une forme informatisée.

[35] François Turenne, *op. cit.*

[36] « Les pharmaciens utilisent depuis bientôt 20 ans des systèmes informatiques pour la saisie de données. Les logiciels ont particulièrement facilité la tâche des professionnels en regard de la facturation à la RAMQ » (Paul Fernet, président de l'Ordre des pharmaciens du Québec, présentation lors du colloque sur *L'informatisation des dossiers de santé : enjeux de droits, enjeux de société*, 9 mai 2001).

Dossiers électroniques centralisés sur une base provinciale

Ce modèle d'entreposage est celui qui est privilégié dans le cadre des récents projets de déploiement de carte santé à microprocesseur au Québec. Le dossier clinique est[37] (ou serait[38]) hébergé à la RAMQ qui en est (ou en serait) le gardien et qui en assure (ou assurerait) la gestion. Se voulant un aide-mémoire pour l'usager, il est à prévoir que ce dossier sera moins précis ou détaillé que le dossier d'établissement ou le dossier électronique centralisés sur une base régionale. Ce modèle, tout comme le précédent, décloisonne les frontières traditionnelles fondées sur le lieu de dispensation de soins. Les organisations de soins ne seront plus ici les gardiens des renseignements cliniques; c'est la RAMQ qui en assurera la garde et l'entretien. Dans ce modèle d'entreposage centralisé sur une base nationale, les points d'alimentation seront plus nombreux et plus étendus que dans le cas du dossier centralisé sur une base régionale. En principe, tous les intervenants de la santé du Québec habilités pourront y accéder et l'alimenter selon des règles d'accès particulières.

2.3 Tendances

Émergence de grands réseaux de renseignements cliniques

Le secteur de la santé est marqué par le développement de réseaux à grande échelle. Le Réseau de télécommunications sociosanitaire (RTSS) et le système de télécommunication interactive entre les pharmacies et la RAMQ en sont présentement deux importantes composantes. Le RTSS relie tous les établissements de santé et de services sociaux du Québec, les 18 régies régionales et leurs technocentres, la RAMQ, l'Office des personnes handicapées du Québec ainsi que le ministère de la Santé et des Services sociaux (MSSS). Comptant au-delà de 1 400 sites répartis sur l'ensemble du territoire québécois,

> [l]e RTSS donne accès à des services communs à plus de 45 000 utilisateurs. Il est aussi possible, pour les télétravailleurs et pour les intervenants externes d'accéder au RTSS par Internet à travers un zone de sécurisation (DMZ). On peut également procéder à des échanges

[37] Projet Laval
[38] Projet Carte d'Accès Santé.

> électroniques avec d'autres réseaux gouvernementaux, ou privés en passant par des passerelles[39].

La Télésanté[40] ainsi que des applications tels le courrier électronique Notes[41] et le système Intégration CLSC utilisent actuellement le RTSS. Selon les orientations technologiques du MSSS (2001), bien d'autres applications se connecteront au RTSS comme le système de Requêtes Résultat Générique, l'Index Patient National, la Carte d'Accès Santé, le Portail Santé et le Dossier Patient Partageable.

Quant au système de télécommunications interactives entre les pharmacies et la RAMQ, il y transite depuis son implantation, le 1er janvier 1997, plus de 50 millions de transactions annuellement afin de gérer en temps réel les demandes de paiement et les autorisations de remboursement des pharmaciens communautaires. Avant l'implantation de ce système interactif, une telle opération de gestion courante prenait une à deux semaines. Elle prend aujourd'hui quelques secondes. Le gouvernement envisage étendre la gestion en direct de la rémunération aux autres professionnels de la santé qui lui chargent des honoraires sur une base régulière, en particulier les médecins.

Un des principaux objectifs poursuivis par le MSSS dans la création et l'interconnexion de réseaux est de rendre accessibles instantanément des renseignements de santé nécessaires à la décision clinique, quels qu'ils soient et où qu'ils soient. Ce réseautage peut prendre aussi bien la forme d'un réseau de dossiers cliniques locaux que d'un réseau de dossiers cliniques centralisés, voire un réseau de dossiers cliniques portables. Les professionnels de la santé pourront alors se communiquer des renseignements cliniques de plus en plus variés et détaillés sur les usagers québécois. En principe, une fois que l'informatisation et la mise en réseau des dossiers cliniques seront complétées, peu d'informations échapperont à l'inforoute de la santé[42].

---

[39] MSSS, *Les orientations technologiques du réseau sociosanitaire. Pour un accès intégré et sécurisé à l'information. Document synthèse*, 2001 : 6.

[40] Présentement, au Québec, la télésanté « répond à des besoins d'échanges spécialisés en cardiologie, en orthophonie, en psychiatrie, en radiologie, en orthopédie, en dermatologie, en télépathologie, en onologie et en formation médicale continue » (*Ibid.* : 7).

[41] « Pour le courrier électronique Notes, plus de 25 000 messages interrégionaux sont transmis chaque jour, en plus des 1 000 à 5 000 messages qui sont envoyés à l'intérieur de chaque région » (*Ibid.* : 6).

[42] Cela pose, entre autres, le problème de la pérennité des accès à cette information. « Plus de 80 % des informations médicales et psychosociales qui ont été produites à mon sujet, au cours de ma vie, sont désormais détruites ou inaccessibles. Par contre, l'enfant qui naîtra en 2005 verra probablement ses informations s'accumuler sur une base continue et perpétuelle – par delà sa propre mort! … Comment s'assurer que les garanties éthiques que nous avons aujourd'hui seront respectées dans 25 ans? » (Pierrot Péladeau, présentation lors du colloque sur *L'informatisation des dossiers de santé : enjeux de droits, enjeux de société*, 9 mai 2001).

Constitution de dossiers cliniques centralisés : deux logiques de développement

L'analyse des précédents projets québécois montre une tendance qui consiste à (vouloir) créer de nouveaux dossiers cliniques à l'extérieur des organisations de soins. Il s'agit de dossiers cliniques centralisés qui sont une réplication en tout ou en partie de dossiers locaux. Par la création de ces dossiers centraux, on ne prétend pas remplacer les dossiers existants. Ces nouveaux dossiers se superposent aux dossiers locaux existants afin de faciliter la circulation de l'information entre les lieux de dispensation de soins et, ainsi, d'améliorer la communication entre les professionnels de la santé. Les sources d'alimentation de ces nouveaux dossiers centralisés se multiplieront au fur et à mesure que se déploiera l'inforoute de la santé, c'est-à-dire l'informatisation et le raccordement des différentes organisations de soins et de services. Parmi les points d'alimentation les plus couramment évoqués, on retrouve les établissements de santé, les cliniques privées, les pharmacies et la RAMQ[43].

Deux logiques semblent sous-tendre le développement de ce nouveau type de dossier : l'une que l'on peut relier à la constitution d'un dossier inter-établissements de type Dossier Patient Partageable, l'autre à la constitution d'un dossier patient de type Dossier Carte Santé. Dans le premier cas, la logique de développement en est une que l'on pourrait qualifier d'hospitalière. Il s'agit d'un dossier qui est sous le contrôle quasi exclusif des professionnels de la santé. La constitution de ce dossier tend à s'inscrire dans un continuum de services (e.g., préhospitalisation, hospitalisation et posthospitalisation) qui se caractérise, entre autres, par un épisode de soins particulier et, donc, par une intensité de services à caractère multidisciplinaire. De plus, en inscrivant des données au dossier de l'établissement, de la clinique ou de la pharmacie, l'intervenant de la santé se trouve du coup à alimenter le Dossier Patient Partageable. Une telle approche évite qu'il y ait double saisie par l'intervenant de la santé. Le consentement de l'usager ne serait pas exigé à chaque accès ou inscription par un tiers afin de ne pas alourdir indûment l'utilisation du Dossier Patient Partageable dans des contextes cliniques particuliers.

[43] Par exemple, le Fichier d'inscription des bénéficiaires servira à alimenter l'Index Patient National alors que le fichier des réclamations, le fichier Med-Écho et le système SIIATH pourraient servir à alimenter le Dossier Patient Partageable et le Dossier Carte Santé en

Quant à la deuxième logique de développement, celle relative au Dossier Carte Santé, elle s'insère davantage dans une approche ambulatoire qui favorise la maîtrise par l'usager de l'information le concernant, que dans une approche hospitalière. Le Dossier Carte Santé s'apparente à un aide-mémoire informatisé, à un dossier minimal électronique géré par le patient, plutôt qu'à un dossier d'établissement géré par des professionnels. Conceptuellement, ce dossier semble moins détaillé que le Dossier Patient Partageable. Contrairement au Dossier Patient Partageable, l'alimentation du Dossier Carte Santé et la communication de son contenu sont sous le contrôle de l'usager. En effet, ce dernier pourra refuser que certains renseignements y soient inscrits ou demander que des renseignements déjà inscrits soient enlevés ou cachés.

Création d'un Index Patient Provincial

Chaque organisation de soins dispose de son propre système d'indexation ou de classement de dossiers. Or, il se crée un nouveau numéro de dossier à chaque fois qu'un usager se présente dans un nouvel établissement. Il arrive parfois qu'un même établissement de santé possède plusieurs numéros de dossiers pour un même usager. Dans ce contexte, l'utilisation d'un identifiant unique semble nécessaire pour permettre la constitution d'un Dossier Patient Réseau ou tout autre regroupement d'information sur un même usager qui proviendrait des différents dossiers locaux existants. Cet identifiant unique semble aussi nécessaire pour identifier de façon fiable et rapide l'usager dans un réseau de soins et de services de plus en plus intégré et informatisé.

L'index Patient Provincial est la solution retenue par le gouvernement pour faciliter la circulation de l'information clinique entre les organisations de santé et pour resserrer l'identification des usagers. Outre l'identifiant unique des usagers, basé sur le numéro d'assurance maladie, l'Index Patient Provincial contiendrait d'autres données d'identification, notamment l'adresse des usagers. Cette information deviendrait accessible à l'échelle du Québec à partir des différentes organisations de soins et de services de santé. Les établissements, les cliniques privées, les pharmacies communautaires et la RAMQ pourraient accéder au contenu de cet index et le mettre à jour. Jusqu'à maintenant, ni la RAMQ, ni le MSSS ou la SOGIQUE n'envisage faire

---

renseignements sur les médicaments prescrits, sur les raisons d'hospitalisation et sur l'historique

intervenir le consentement de l'usager quant à l'accès et à la mise à jour de l'Index Patient Provincial.

2.4 Enjeux relatifs à l'inforoute de la santé

Concentration des données ou interconnexion des dossiers

La concentration des données cliniques peut inquiéter. Cela n'est pas étranger au fait que les risques qui y sont associés sont considérables.

> [S]i la puce électronique est plus sûre que le papier, le fait de dévaliser un entrepôt de données numérisées et personnalisées, ou le fait de bloquer l'accès à un site de données, alors qu'on en a besoin, peuvent avoir des conséquences plus considérables que celles que comporte l'usage des dossiers papier[44].

Une seule brèche, une seule fuite peut être lourde de conséquences, voire catastrophique. Nous sommes en droit de penser que l'ampleur des conséquences d'un bris de confidentialité augmentera avec le degré de concentration des données cliniques. Les deux modèles d'entreposage de dossiers cliniques centralisés, l'un couvrant une région, l'autre la province, comportent de tels risques. Quant au modèle basé sur l'interconnexion des dossiers locaux, il n'est pas exempt de tout risque. Chaque organisation connectée au réseau devient autant de porte d'entrée à sécuriser. Il devra y avoir autant de gardiens de l'information qu'il y aura de lieux d'entreposage. Dans la mesure où l'ampleur des risques augmente avec le degré d'informatisation et d'interconnexion, il devient, entre autres, important d'identifier et d'authentifier les utilisateurs du réseau d'information, tout en s'assurant de l'intégrité des renseignements que ceux-ci inscrivent aux dossiers et de la non-répudiation de ce qu'ils ont inscrit.

Gestionnaire et gardien de dossiers cliniques réseautés

La concentration des données cliniques inquiète d'autant plus qu'elle concerne le plus gros assureur dans le secteur de la santé au Québec, la RAMQ. Cette organisation

---

des transfusions sanguines.

détient et gère déjà d'importantes banques de renseignements de nature clinique : Med-Écho, réclamations des médicaments, services médicaux rémunérés, Hygiène mentale, Registre des traumatismes, Fichiers des tumeurs, Intégration CLSC, etc. Elle détient aussi un identifiant unique, le numéro d'assurance maladie, qui lui permet de croiser ces banques. Cette concentration de l'information préoccupe bon nombre de personnes[45] et d'organismes[46] qui voient là une ingérence des appareils administratifs de l'État dans la relation clinique entre l'usager et le professionnel. Il y a lieu aussi de s'inquiéter de l'intention gouvernementale d'étendre le pouvoir de collecte et d'entreposage de la RAMQ à des renseignements cliniques relatifs à des services non assurés par l'État, en particulier les données « relatives aux personnes non assurées par la Régie dans le cadre du régime d'assurance-médicaments »[47]. À l'instar de plusieurs agents sociaux (organismes communautaires, associations et ordres de professionnels, journalistes, chercheurs, etc.), nous croyons qu'il est important de dissocier dans la mesure du possible le rôle d'assureur ou d'agent payeur de celui de gestionnaire et dépositaire de dossiers cliniques.

Dans le cas de la Carte D'Accès Santé, le ministre de la Santé et des Services sociaux soutient que la RAMQ mettra en place une architecture technologique qui érigera une cloison étanche entre l'« administratif » et le « clinique ».

> L'infrastructure technologique sur laquelle repose l'utilisation de la *Carte d'Accès Santé à microprocesseur* est conçue de manière à distinguer ces deux fonctions … les renseignements personnels de nature médicale portés au *Dossier Carte Santé* de l'usager et conservés en fiducie à la Régie ne pourront être utilisés à des fins autres que pour lui dispenser des soins de santé. Un cadre juridique devra prévoir notamment l'interdiction à

---

[44]Collège des médecins, mémoire déposé au Colloque sur les orientations stratégiques du MSSS, juin 2000.

[45] Voir notamment les articles suivants : Robert Dutrisac, *Le Devoir* du 30 avril 2001, Vers un relevé individuel du coût des soins de santé. Trudel fait miroiter tous les bénéfices d'une carte à puce; Brigitte Breton, dans *Le Soleil* du 2 mai 2001, Le bon usage d'une carte; Pierrot Péladeau, dans *Le Devoir* du 2 mai 2001, Carte santé à microprocesseur : l'incontournable débat public.

[46] Plusieurs représentants d'organismes communautaires et autres organismes, invités au Colloque du 9 mai 2001 sur *L'informatisation des dossiers de santé : enjeux de droits, enjeux de société,* ont exprimé des craintes quant à la constitution d'un dossier clinique centralisé à la RAMQ.

[47] Ministre Trudel, mémoire déposé au Conseil des ministres, *op. cit.* : 5. À cet égard, voir l'avis de la Commission d'accès à l'information portant sur les "Mesures structurantes pour améliorer le fonctionnement et accroître l'efficacité du Régime général d'assurance médicaments", 16 janvier 2001.

> un assureur, même public, ou à un employeur d'avoir accès au *Dossier Carte Santé* de cette personne[48].

La cloison entre l'administratif et le clinique sera-t-elle vraiment étanche? Sur le plan légal, l'expérience des dernières années nous montre au contraire que le gouvernement a tendance à apporter des amendements aux lois et à y inclure des exceptions quant à l'utilisation et à la communication de renseignements personnels afin de poursuivre diverses finalités ou de répondre au besoin de différents organismes[49]. Sur le plan technologique, il est difficile d'imaginer que la RAMQ, principal gestionnaire des banques de données du secteur de la santé, veuille détenir une banque de renseignements sans se donner les moyens de la gérer, notamment sur le plan de l'intégrité et des accès. De plus, comment gérer le renouvellement des cartes sinon en gardant une copie de celle-ci et, par conséquent, de tous les trousseaux de clés du Dossier Carte Santé. La RAMQ détiendra-t-elle les trousseaux de clés qui lui donneront accès de façon nominative à tout le contenu du Dossier Carte Santé?[50] Détiendra-t-elle à la fois le coffre fort et les clés du coffre?

D'autre part, est-il plus sécuritaire de centraliser le dossier à l'échelle régionale, comme le souhaitent les partisans d'un Dossier Patient Partageable? Là aussi, le problème de la centralisation des renseignements cliniques demeure entier dans la mesure où la majorité de la population québécoise consomme la plupart de ses services de santé dans la région où elle réside. Du point de vue de l'usager, la centralisation des renseignements de santé au niveau régional peut ressembler à une centralisation au niveau national, un dossier régional pouvant être aussi complet qu'un dossier national.

Présentement, la garde des dossiers locaux est sous la responsabilité d'entités légales bien circonscrites, comme l'établissement, la clinique privée ou la pharmacie, et sous la surveillance de gardiens bien identifiés que sont le directeur des services professionnels, l'archiviste ou la secrétaire médicale. En contribuant au décloisonnement des systèmes de soins et d'information, l'avènement de l'inforoute, conjugué au virage ambulatoire, risque de bousculer les habitudes quant à la conservation des dossiers et à la gestion de leur accès. Qui aura les responsabilités de gardien ou de gestionnaire d'un éventuel

---

[48] Mémoire déposé au Conseil des ministres … annexe I : 2.
[49] L'article 65 de la Loi sur l'assurance-maladie en est un exemple éloquent.

dossier centralisé réseauté? Est-ce que ce sera la RAMQ? les technocentres régionaux? les CHU? Présentement, aucune de ces entités légales n'est habilitée à assurer la garde d'un tel dossier.

Index Patient National

Selon le ministre de la Santé et des Services sociaux, le personnel d'une organisation de soins pourra accéder à un Index Patient National « en tout temps et en toutes circonstances … sans la présence de la personne concernée »[51]. L'Index Patient National donnera accès, comme nous l'avons dit, à des données d'identification telles que le nom, le prénom et l'adresse. Il contiendra aussi les numéros de dossiers des usagers de ces organisations de soins. Ce système est préoccupant du fait qu'il repose sur la mise en réseau des données d'un fichier de renseignements personnels centralisé à la RAMQ, le Fichier d'inscription des bénéficiaires (FIB). Cela revient à créer un registre ou bottin provincial contenant les noms et les adresses de tous les citoyens du Québec. Il y a lieu de questionner la légitimité et la nécessité de diffuser à grande échelle un tel méga fichier. La mise en réseau d'un tel fichier sur la population québécoise est-elle indispensable à la circulation de renseignements cliniques dans le secteur de la santé? Cette préoccupation est d'autant plus à propos que les risques de fuites s'accroissent au fur et à mesure qu'augmentent le nombre d'utilisateurs et la grosseur des fichiers. En effet, l'expérience nous montre qu'il est difficile de restreindre et de contrôler les accès par des mesures de sécurité efficaces lorsque les utilisateurs sont nombreux.

---

[50] La création par la RAMQ d'un fichier de sauvegarde de tout le contenu des cartes d'usager met sérieusement à l'épreuve l'étanchéité entre la RAMQ et les données cliniques nominatives du Dossier Carte Santé.

[51] Rémy Trudel, mémoire déposé au Conseil des ministres, *op. cit.*

3. CADRE JURIDIQUE QUÉBÉCOIS CONCERNANT LES RENSEIGNEMENTS DE SANTÉ

Les règles québécoises en matière de protection des renseignements personnels concernant la santé sont nombreuses, éparpillées, parfois contradictoires et, sous certains aspects, insuffisantes dans le contexte de l'implantation des nouvelles technologies de la santé. Les décrire de façon exhaustive permettrait sans contredit de démontrer un tel constat. Toutefois, l'exposé qui suit s'attarde uniquement aux dispositions légales qui s'appliquent aux organismes publics instigateurs des projets québécois décrits plus haut, c'est-à-dire les centres hospitaliers, les CLSC, les régies régionales, la RAMQ et le MSSS.

3.1 Lois d'application générale

Au Québec, plusieurs dispositions législatives de nature générale imposent le droit au respect de la vie privée et de la protection des renseignements personnels, que ces renseignements soient de nature médicale ou non. La *Charte des droits et libertés de la personne* (L.R.Q. chapitre C-12) énonce expressément que toute personne a droit au respect de sa vie privée. Quant à la *Charte canadienne*, elle reconnaît que toute personne a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Selon la Cour suprême du Canada, cette disposition constitutionnelle garantit également une protection de la vie privée. Le *Code civil du Québec* confirme ce droit et y ajoute plusieurs règles relatives à la protection des renseignements personnels.

Pour ce qui est de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès, L.R.Q., chapitre A-2.1), elle s'applique à tous les organismes publics québécois, dont les établissements de santé et de services sociaux, la RAMQ, les régies régionales et le MSSS. Cette loi, qui a un caractère prépondérant sur toutes les autres, offre des garanties de protection des renseignements personnels que l'on peut qualifier de « minimales ». Ainsi, une autre loi peut renforcer la règle de confidentialité des renseignements personnels, auquel cas la règle la plus sévère devra s'appliquer. Tel est le cas pour la *Loi sur les services de santé et les services sociaux* (LSSSS, L.R.Q., chapitre S-4.2) qui limite davantage que ne le fait la Loi sur l'accès les possibilités de communication des renseignements de santé à des tiers sans le consentement des personnes concernées. Il faut également

mentionner, même si elle ne s'applique pas aux organismes publics, que la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le secteur privé, L.R.Q., chapitre P-39.1) établit la conduite que doivent respecter les entreprises du secteur privé. Cette loi doit être respectée par les cliniques médicales, les laboratoires privés, les cabinets de dentistes, les pharmacies communautaires, les organismes de recherche privés, etc.

Les lois professionnelles, tels le *Code des professions* (L.R.Q., chapitre C-26) et la *Loi médicale,* (L.R.Q., chapitre M-9) reconnaissent également l'obligation de respecter le secret professionnel. D'autres obligations de même nature sont également prévues par les codes de déontologie adoptés par la vingtaine d'ordres professionnels œuvrant dans le secteur de la santé. Cependant, ces dispositions ne s'appliquent qu'aux professionnels et non aux organismes publics.

Récemment adoptée par l'Assemblée nationale, la *Loi concernant le cadre juridique des technologies de l'information* (L.Q., 2001, chapitre 32) amènera aussi l'ensemble des organismes, publics ou privés, à prendre des mesures pour assurer la sécurité des communications peu importe le support des documents utilisés. Des règles seront prévues pour assurer l'intégrité de l'information, la responsabilité des intermédiaires sur les réseaux de communication, l'authentification de l'identité d'une personne, etc.

3.2 LSSSS et Loi sur l'accès

Un chapitre particulier de la LSSSS s'attarde à énoncer les règles de confidentialité applicables au dossier de l'usager. Ce chapitre ne s'applique cependant qu'aux établissements de santé et de services sociaux : CLSC, centre hospitalier, centre de protection de l'enfance et de la jeunesse, centre d'hébergement et de soins de longue durée et centre de réadaptation. En outre, si une disposition de ce chapitre est inconciliable avec une autre règle prévue par la Loi sur l'accès, la première aura préséance. Quant aux régies régionales et au MSSS, ils doivent répondre aux exigences de la Loi sur l'accès en matière de confidentialité des renseignements personnels.

La LSSSS et la Loi sur l'accès établissent donc le principe de la confidentialité du dossier de l'usager et des renseignements personnels. Comme toute règle générale, ces deux lois souffrent toutefois de quelques exceptions, ces dernières étant moins

nombreuses dans la LSSSS. Assurant donc une plus grande confidentialité des renseignements personnels, seule la LSSSS s'applique aux renseignements du dossier de l'usager.

Exceptions à la règle de la confidentialité

Les exceptions à la règle de la confidentialité du dossier de l'usager détenu par un établissement de santé et prévues par la LSSSS sont les suivantes :

- il y a consentement de l'usager ou d'une personne qui peut consentir à sa place (art. 19);
- sur l'ordre d'un tribunal ou d'un coroner dans l'exercice de ses fonctions (art. 19);
- lorsque la LSSSS (et non pas n'importe quelle loi) l'autorise (art.19). Par exemple :
    - les héritiers, représentants légaux, conjoints, ascendants et descendants peuvent, dans certaines circonstances, avoir accès à des renseignements contenus dans le dossier d'un usager décédé (art. 22 et 23);
    - le directeur des services professionnels d'un établissement autorise la communication à des fins d'étude, d'enseignement ou de recherche (art. 19.1);
    - un accès limité est accordé lors de l'examen d'une plainte formulée par un usager (art. 38);
    - l'accès aux renseignements est nécessaire pour permettre à un ordre professionnel, un inspecteur du MSSS ou un enquêteur du gouvernement d'exercer les pouvoirs que la LSSSS leur confie (art. 77, 489 et 500);
    - lorsque le Conseil des médecins, dentistes et pharmaciens de l'établissement a confié à un expert externe un mandat pour contrôler ou évaluer la qualité des actes médicaux, dentaires ou pharmaceutiques ou encore la compétence des professionnels appelés à poser ces actes (art. 214).

Quant à la Loi sur l'accès, elle regroupe, à l'article 59, les exceptions à la règle de confidentialité des renseignements personnels détenus par les autres organismes

publics, dont les régies régionales et le MSSS. Aussi est-il possible de communiquer de tels renseignements sans le consentement de la personne concernée, entre autres dans les situations suivantes :

- la communication est nécessaire à l'application de n'importe quelle loi au Québec;
- la communication est nécessaire à l'exercice d'un mandat confié par l'organisme public à une autre personne ou organisme;
- la communication est nécessaire 1) à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont cet organisme public a la gestion; 2) lorsque des circonstances exceptionnelles le justifient; 3) à l'application d'une loi au Québec et que cette communication implique le couplage de fichiers de renseignements personnels. Dans tous ces cas, une entente doit être conclue avant la communication et cette entente doit être soumise pour avis à la Commission d'accès à l'information;
- les renseignements sont requis par le procureur de l'organisme ou par une personne chargée de prévenir, détecter ou réprimer une infraction à une loi applicable au Québec, mais uniquement lorsque certaines conditions sont réunies;
- lorsque la Commission d'accès à l'information accorde une autorisation de communication de renseignements personnels à des fins d'étude, de recherche ou de statistique.

Règles particulières de collecte de renseignements personnels par le MSSS et les régies régionales

Afin de préserver le caractère confidentiel des renseignements contenus dans le dossier de l'usager, le législateur a considérablement limité la possibilité pour les régies régionales et le MSSS de recueillir des renseignements personnels consignés dans les dossiers des usagers détenus par les établissements. La LSSSS traduit cette intention du législateur de la façon suivante :

- lorsqu'une régie régionale exerce ses fonctions reliées aux priorités de santé et de bien-être, il lui est interdit de colliger tout renseignement ou document permettant d'identifier un usager (art. 381);

- que ce soit pour ses propres fins ou celles du ministre, une régie régionale, qui exige des établissements de l'information concernant les clientèles, les services et les ressources, ne peut recueillir des renseignements qui pourraient permettre l'identification d'un usager (art. 381);

- si une régie régionale fournit, à la demande du ministre, des états, données statistiques, rapports et autres renseignements sur ses activités, elle ne peut fournir des renseignements qui pourraient permettre d'identifier un usager (art. 394);

- dans l'exercice de ses fonctions, le ministre (et non la régie régionale) peut requérir qu'un établissement lui fournisse les renseignements personnels ou non qui concernent les besoins et la consommation de services. Toutefois, cette collecte doit être autorisée par un règlement adopté par le gouvernement. À ce jour, trois règlements autorisent la collecte de renseignements personnels par le ministre. Ces règlements autorisent les établissements à communiquer au ministre des données relatives aux hospitalisations, aux personnes ayant subi un traumatisme majeur ou ayant reçu une transfusion sanguine ou des produits sanguins (art. 433 et 505(26)) [52].

Toutes les dispositions législatives décrites ci-dessus confirment l'importance que la société accorde à la confidentialité des renseignements relatifs à la santé des individus. Toutefois, le principe de confidentialité n'est pas le seul à assurer la protection des renseignements personnels. En effet, d'autres principes, qui seront décrits plus loin, s'appliquent à la collecte, à l'utilisation, à la communication, à la conservation et à la destruction des renseignements personnels.

3.3 Des règles juridiques adéquates?

L'informatisation du dossier clinique et sa circulation sur une éventuelle inforoute soulèvent plusieurs questions de nature juridique dont il serait trop long ici de faire une analyse exhaustive. Il demeure que les réponses qui seront apportées à certaines de ces questions auront un impact majeur sur la protection des renseignements personnels et

[52] Les règlements dont il est question sont le *Règlement sur l'organisation et l'administration des établissements de santé et de services sociaux* (L.R.Q., c. S-5, r.3.01, art. 19); le *Règlement sur la transmission de renseignements concernant les personnes ayant reçu une transfusion*

de la vie privée. Ainsi, les avancées importantes des technologies de l'information et, plus particulièrement, de la mise en réseau des renseignements de santé suscite une sérieuse réflexion sur la protection des renseignements personnels que les Québécoises et Québécois veulent voir accorder aux renseignements qui les concernent.

Du serment d'Hippocrate à la LSSSS, la sensibilité des renseignements relatifs à la santé a toujours été largement reconnue et les règles de confidentialité ajustées en conséquence. Avant de remettre en cause de tels principes, il semble à tout le moins que le législateur devrait clairement exprimer quelles sont les nouvelles règles du jeu. Or, jusqu'à preuve du contraire, l'article 19 de la LSSSS trace clairement la conduite à suivre : les renseignements contenus dans le dossier d'un usager sont confidentiels et ils ne peuvent être communiqués qu'avec le consentement de cet usager ou si l'une des exceptions de la LSSSS trouve application.

Des règles qui varient selon le détenteur de l'information

Depuis quelques années, grâce entre autres aux possibilités offertes par l'informatique et la télématique, nous constatons que le même renseignement de santé reçoit un traitement différent selon le détenteur de l'information. Par exemple, dès qu'un établissement communique au ministre de la Santé et des Services sociaux un renseignement relatif à l'hospitalisation d'un usager, conformément à un règlement validement adopté, ce renseignement n'est plus protégé par les règles de confidentialité de la LSSSS. Il peut être communiqué selon les règles prévues par la Loi sur l'accès, laquelle autorise davantage de dérogations à l'interdiction de communiquer des renseignements sans le consentement de la personne concernée, comme nous l'avons mentionné précédemment. Ainsi, une fois en sa possession, le MSSS peut communiquer le renseignement de santé à un autre organisme, par exemple la RAMQ, afin de procéder à des couplages de fichiers. En outre, ces mêmes renseignements peuvent être communiqués à un mandataire ou à un corps de police. Cet exemple montre l'importance de se poser la question suivante et d'y répondre : les règles de

---

sanguine ou des produits sanguins (L.R.Q., c. S-4.2, r.8) et le *Règlement sur la transmission de renseignements concernant les usagers victimes de traumatismes majeurs* (L.R.Q., c. S-4.2, r.9)

protection d'un renseignement de santé devraient-elles être différentes d'un détenteur du renseignement à un autre?[53]

Quant à la détention par les régies régionales de renseignements concernant les usagers, la LSSSS est très claire : les régies régionales ne peuvent obtenir de renseignements permettant d'identifier un usager. Doit-on conclure que les régies n'auront aucun accès aux renseignements de santé qui seront appelés à circuler sur l'inforoute de la santé, peu importe l'utilisation que pourraient en faire les régies?

Détenteurs des renseignements de santé

Présentement, les projets québécois liés à la mise en réseau des renseignements de santé laissent entrevoir qu'un nombre de plus en plus grand d'organismes ou de personnes auront accès à ces renseignements, que ce soit avec le consentement de la personne concernée ou sans celui-ci. MSSS, RAMQ, régies régionales, technocentres locaux, régionaux ou national, établissements de santé, organismes communautaires pourront en certaines circonstances avoir accès aux renseignements de santé.

Par ailleurs, les fusions de certains établissements de santé et de services sociaux aux vocations variées modifient considérablement les modalités des échanges de renseignements entre ces établissements. Le même constat vaut pour la nouvelle approche de distribution des soins axée sur le mode ambulatoire. Pour un épisode de soins, plusieurs établissements veulent avoir accès aux renseignements concernant l'usager concerné.

Or, le contexte légal des nouvelles organisations de soins et le statut juridique des intervenants, y compris le MSSS, la RAMQ et les régies régionales, sont pour l'instant imprécis : qui devient le détenteur juridique ou le détenteur physique de l'information partagée sur une base régionale ou nationale? Quel organisme sera responsable d'assurer la sécurité des informations? S'agira-t-il d'une responsabilité partagée? Qui devra s'assurer du respect des règles de confidentialité? À qui devra s'adresser la personne qui veut avoir accès à son dossier ou formuler une demande de rectification de renseignements qui sont inexacts, incomplets ou univoques? Qui devra faire la

[53] Cette question ne concerne que les règles établies dans le secteur public. La législation applicable par le secteur privé soulève également des questions de même nature.

déclaration de fichiers de renseignements personnels à la Commission d'accès à l'information? S'il doit absolument y avoir concentration d'information, qui assumera cette responsabilité et quelles règles juridiques l'encadreront? Quelles sont les règles de transparence qui permettront aux Québécois de connaître tout le chemin suivi par les renseignements qui les concernent? Les réponses à ces questions ne sont pas sans importance puisqu'elles détermineront les responsabilités des divers intervenants eu égard aux obligations qu'ils doivent respecter en vertu de la Loi sur l'accès.

3.4 Principes de protection des renseignements personnels

L'analyse des projets québécois de mise en réseau des dossiers cliniques nous permet de pointer les difficultés juridiques sans pour autant pouvoir y apporter toutes les réponses. Sans présumer des solutions qui pourraient être retenues, il faut signaler que toutes les lois occidentales de protection des renseignements personnels sont fondées sur de grands principes, traduits par chaque pays par des mesures législatives qui peuvent varier. Le respect de ces principes ne devrait pas être remis en cause par la mise en réseau de l'information clinique. Ces principes s'appliquent aux différentes étapes de la vie d'un renseignement personnel : sa collecte, son utilisation, sa communication, sa conservation et sa destruction.

Principe de la finalité

Au moment de la collecte d'un renseignement, un organisme doit informer la personne concernée des fins auxquelles est destiné le renseignement. L'analyse des projets québécois permet d'identifier trois finalités bien différentes : clinique, administrative et scientifique (recherche). Si un renseignement est collecté à des fins cliniques, il ne devrait pas servir à des fins administratives ou de recherche à moins que la personne concernée y consente ou qu'une loi l'autorise. Tel est le cas de la LSSSS et de la Loi sur l'accès qui prévoient la possibilité d'obtenir des autorisations de recherche du directeur des services professionnels, si les renseignements sont détenus par un établissement de santé, ou par la Commission d'accès à l'information si les renseignements sont détenus par un autre organisme public.

Principe de la nécessité

Seuls les renseignements nécessaires à la réalisation des finalités déclarées pourront être recueillis et utilisés. Le principe de nécessité permet d'éviter la collecte tous azimuts de renseignements qui pourraient alimenter des banques de données dans l'éventualité où ces renseignements pourraient être utiles un jour. À l'ère de l'informatique et de la télématique, certains souhaiteraient se servir de ces nouveaux outils conviviaux pour collecter non seulement les renseignements nécessaires, mais aussi tous ceux qui peuvent être recueillis. Le principe de la nécessité interdit une telle pratique.

Il faut convenir que le principe de la nécessité, aussi important soit-il, peut parfois porter à confusion. Comment déterminer si un renseignement est nécessaire ou pas pour atteindre un objectif précis? Cet exercice est d'autant plus complexe que la collecte des renseignements ne doit simplement être utile mais bien nécessaire, au sens d'indispensable.

Dans le secteur de la santé, l'application du critère de la nécessité ne va pas sans soulever plusieurs questions propres à ce secteur. Bien souvent, le renseignement devra être colligé avant même que le professionnel de la santé ne puise en déterminer la nécessité. Le contexte de chaque situation doit donc être pris en considération pour évaluer la nécessité de la collecte d'un renseignement relatif à la santé d'un individu.

S'il apparaît que le renseignement relatif à la santé d'un individu n'est pas nécessaire aux fins pour lesquelles il est recueilli, sa collecte est alors interdite. L'obtention d'un consentement de cet individu ne permettra pas contourner cette règle de la nécessité.

Principe de la confidentialité

La confidentialité d'un renseignement personnel est essentielle au respect du droit à la vie privée et à la protection des renseignements personnels. Sans l'assurance du maintien de cette confidentialité, le lien de confiance qui doit s'établir entre un individu et l'organisme ou l'intervenant qui collecte les renseignements peut être rompu. Dans le secteur de la santé, ce principe est d'autant plus important qu'un usager pourra refuser de communiquer des renseignements essentiels à un professionnel de la santé si les garanties de confidentialité sont déficientes. Lorsqu'une personne manipule au sein d'un organisme public un renseignement aux fins de l'exercice de ses fonctions, elle doit

s'assurer qu'elle agit de façon à sauvegarder sa confidentialité. Par ailleurs, la communication de ce renseignement à un tiers est interdite à moins que la personne concernée n'y ait consenti ou qu'une telle communication soit autorisée par la loi. Pendant la durée de conservation, l'organisme doit également s'assurer que la confidentialité de l'information est maintenue. Pour atteindre tous ces objectifs, des mesures de sécurité adéquates devront évidemment être appliquées.

Principe de la durée limitée de conservation

Lorsque les fins pour lesquelles le renseignement a été recueilli sont accomplies, ce dernier devrait être détruit. Au Québec, diverses mesures obligent les organismes publics à établir des calendriers de conservation de leurs documents. Le fait que ces documents soient consignés sur un support informatique ou qu'ils soient mis en réseau n'atténue en rien l'obligation de respecter le calendrier de conservation. Ce principe est étroitement relié à la règle du droit à l'anonymat [the right to be let alone] qui fonde le droit à la vie privée.

Principe du respect des droits d'accès et de rectification

Peu importe les modes de collecte, d'utilisation, de communication ou de conservation des renseignements, les personnes concernées doivent toujours pouvoir exercer leurs droits d'accès et de rectification. Ce principe est essentiel pour permettre aux individus d'exercer un contrôle sur la communication à des tiers des renseignements qui les concernent. Les technologies de l'information, mises en place pour emmagasiner les renseignements de santé et pour faciliter leur circulation, ne doivent pas constituer un obstacle à l'exercice de ces droits.

Principes de protection et de transparence

Le respect de l'ensemble des principes décrits ci-dessus ne peut être atteint que si les organismes prennent des mesures pour assurer la protection des renseignements personnels ainsi que la transparence de l'utilisation des renseignements personnels qu'ils détiennent. L'organisme doit, entre autres, déclarer le sort qui sera réservé aux renseignements qu'il collecte et qu'il conserve.

4. CONSENTEMENT

Le consentement est un gage de respect de la volonté de l'individu face à sa vie privée. À moins d'exceptions prévues par le législateur, le consentement est incontournable lors de la collecte de renseignements personnels, de leur utilisation à des finalités non déclarées ou de la communication à des tiers. En principe, il est doit être présent aux différentes étapes de la vie d'un renseignement personnel. Cependant, comme nous le verrons dans ce dernier chapitre, le consentement ne peut reposer sur une mécanique fixe et rigide quand il s'agit de renseignements personnels de santé utilisés à des fins cliniques dans un contexte d'inforoute.

4.1 Transparence et maîtrise des accès par l'usager

Avec l'informatisation des dossiers cliniques et leur mise en réseau, les renseignements de santé sur les usagers seront désormais plus facilement accessibles, quel que soit le modèle d'architecture retenu. L'inforoute permettra non seulement de repérer la localisation des dossiers cliniques sur un même individu[54], mais aussi d'y accéder, de traiter l'information qui s'y trouve et de la mettre à jour, et ce de façon quasi instantanée. L'information réseautée sera de plus en plus complète. Sans la mise en place de mécanismes de consentement appropriés, l'inforoute de la santé pourrait devenir une entrave à la capacité de l'usager à préserver son intimité et à s'affranchir de son passé. Alors que l'usager a encore aujourd'hui le loisir de changer d'hôpital, de clinique ou de pharmacie pour ne pas être reconnu et être oublié, cette liberté pourrait disparaître avec l'avènement d'une inforoute de la santé dont les phases de conception et d'implantation auraient été menées de façon précipitée, sans les garanties de confidentialité nécessaires. Son dossier clinique pourrait le suivre où qu'il aille dans le système de santé. L'usager voudra-t-il toujours tout divulguer sur son état santé actuel et, surtout, sur ses antécédents de maladies, même lorsqu'il consulte un médecin? L'usager pourra-t-il demander un deuxième avis médical sans que l'un ou l'autre des médecins consultés le sache? Pourra-t-il cacher à un médecin qu'il ne connaît pas, consulté pour une entorse dans une clinique sans rendez-vous ou à

[54] Plus la localisation du dossier à partir de l'index est précise et explicite, plus elle peut nous renseigner sur la nature clinique des dossiers. Les dossiers associés à des départements de psychiatrie en sont un exemple éloquent.

l'urgence, qu'il a déjà pris des antidépresseurs, qu'il a déjà eu un cancer, un avortement ou des problèmes d'alcoolisme?

Dans un contexte d'inforoute où les renseignements de santé personnels circuleront plus facilement et instantanément, l'usager devra plus que jamais demeurer le maître de son information. Plus précisément, il devra continuer à exercer dans la mesure du possible un contrôle sur l'accès par des tiers aux renseignements cliniques le concernant. Ce n'est pas parce qu'il y a mise en réseau des dossiers que l'autorisation de l'usager à communiquer de l'information à des professionnels doit cesser. Au contraire, ce consentement sera d'autant plus requis qu'il donnera accès à des renseignements plus nombreux, provenant de différents lieux de dispensation de soins. Comme le signalent les archivistes

> c'est un droit absolu de l'usager que de consentir ou non à un transfert d'information le concernant, de limiter le contenu de l'information divulguée, de nommer les personnes autorisées à accéder à cette information et de donner les délais limitant l'accès dans le temps[55].

L'efficacité de l'inforoute de la santé dépend de la confiance des utilisateurs dans les mesures de sécurité qu'offre le système. Des garanties de sécurité insuffisantes inciteraient les utilisateurs de ce système, aussi bien les usagers que les professionnels, à ne plus l'alimenter. D'une part,

> si un malade soupçonne que des informations fournies à son médecin peuvent être rendues disponibles à d'autres sans son consentement, il peut choisir de redoubler de prudence, voire de conserver désormais pour lui-même des renseignements qu'il aurait dû partager avec son médecin[56].

D'autre part, en reconnaissant à l'usager le pouvoir de contrôler la communication de ses renseignements cliniques réseautés, ne risquons-nous pas d'ébranler la crédibilité de l'information disponible? Or, il est raisonnable de soutenir que, de façon générale, les usagers consentiront à la communication d'information de santé les concernant s'ils jugent qu'un telle communication leur sera cliniquement bénéfique. Il est aussi raisonnable de reconnaître à l'usager le pouvoir de garder secrètes certaines informations qui concernent des événements cliniques du passé et qui n'ont plus d'utilité clinique dans le cadre d'un problème donné ou d'un épisode de soins

---

[55] Mémoire déposé au Colloque sur les orientations stratégiques du MSSS, juin 2000.
[56] Collège des médecins (2000), *op. cit.*

particulier, et ce sans perdre la confiance du professionnel qui le soigne. Il est important ici de distinguer, d'une part, la mise à jour des dossiers cliniques locaux, qui est obligatoire et sur laquelle l'usager exerce très peu de contrôle, et, d'autre part, l'accès à distance au contenu de ces dossiers à partir de l'inforoute, sur lesquels l'usager devrait exercer un certain contrôle. Autrement dit, si l'usager ne peut empêcher l'inscription dans son dossier de santé de renseignements cliniques qui résultent d'une rencontre entre lui et un professionnel de la santé, il doit exercer un certain contrôle sur la circulation de ces renseignements dans un contexte d'inforoute.

4.2 Validité du consentement

Selon l'article 19 de la LSSSS,

> 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, sur l'ordre d'un tribunal ou d'un coroner dans l'exercice de ses fonctions ou dans le cas où la présente loi prévoit que la communication de renseignements contenus dans le dossier peut être requise d'un établissement.

La Loi sur le secteur privé prévoit, à l'article 14, une disposition sur la validité du consentement à la communication[57].

> Le consentement à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Plus précisément, la Commission d'accès à l'information définit les principes de validité du consentement de la façon suivante :

1) Le consentement doit être manifeste, c'est-à-dire un geste clair et explicite : la personne sait qu'elle consent;
2) le consentement doit être libre, c'est-à-dire un geste volontaire qui ne fait pas l'objet de pression ou de discrimination : l'usager peut consentir en toute confiance;

[57] Une disposition similaire sera probablement applicable pour le secteur public lorsque l'article 11 du projet de loi n^{o} 122, modifiant l'actuelle Loi sur l'accès, aura été adopté.

3) le consentement doit être éclairé de manière à ce que la personne sache à qui (tiers) et à quoi (contenu) elle consent : l'usager consent en connaissance de cause;
4) le consentement doit être donné à des fins spécifiques pour une durée limitée afin d'éviter, entre autres, des utilisations secondaires non prévues : l'usager sait pourquoi et pour combien de temps il consent.

Dans l'univers papier, les principes de validité du consentement peuvent s'appliquer sans trop de difficultés à la communication de renseignements de santé entre des organisations de soins distincts. De plus, les règles d'accès et les gardiens de l'information[58] sont connus et reconnus officiellement. Ces principes s'appliqueront-ils de la même façon dans le cadre de l'inforoute de la santé, voire à l'intérieur d'un même établissement de santé informatisé qui aurait fusionné avec d'autres établissements? Le consentement sera-t-il exigé à la pièce, chaque fois que le professionnel utilisera l'inforoute pour accéder à un dossier clinique réseauté? Le consentement sera-t-il étendu dans le temps et dans l'espace? Comment gérer le consentement dans une architecture de banques centralisées? L'intervenant de la santé aura-t-il toujours besoin de toute l'information clinique disponible sur l'inforoute? L'usager pourra-t-il décider, dans des circonstances précises, des renseignements qu'il désirera divulguer au professionnel?

4.3 Scénarios de consentement

À certains égards, le déploiement de l'inforoute de la santé met à l'épreuve les principes de validité du consentement ainsi que les règles habituelles de fonctionnement qui les appuient. Afin de mieux cerner la portée et les limites d'un consentement valide dans un contexte d'inforoute, nous l'avons confronté à trois situations cliniques particulières : les problèmes de santé ponctuels non urgents, les épisodes de soins et les situations d'urgence. Nous ne prétendons pas que ces situations cliniques soient exhaustives. Il faudrait y ajouter les problèmes chroniques, les maladies dégénératives et bien d'autres problèmes de santé. Par l'examen de ces trois situations cliniques, nous cherchons essentiellement à montrer qu'un consentement valide renvoie

[58] Archiviste, directeur des services professionnels, secrétaire médicale et professionnel de la santé.

non pas à une mécanique fixe, mais à des règles qui doivent s'adapter à des situations cliniques particulières tout en tenant compte des capacités des réseaux électroniques.

Problèmes de santé ponctuels non urgents

Au cours de sa vie active, l'individu moyen aura consulté des médecins, des pharmaciens et autres professionnels pour des problèmes de santé ponctuels, souvent mineurs et sans conséquences graves, qui se règlent à la suite de quelques consultations, parfois une seule. Dans ce cas-ci, le professionnel n'a souvent pas besoin de connaître le passé clinique de l'usager dans le détail pour prendre une décision éclairée; la parole de l'usager peut suffire en autant que celui-ci a la capacité de se raconter et de rendre compte de son état de santé de façon intelligible. De plus, l'usager peut avoir ses raisons de ne pas divulguer des éléments de son passé. Dans ce contexte clinique, nous croyons que le consentement doit être manifeste (un geste clair et explicite), libre (préserver la relation de confiance) éclairé (savoir qui a accès à quoi et quand) et spécifique (d'une portée et d'une durée limitées). Ici, plus qu'ailleurs, l'usager devra continuer à exercer un certain contrôle sur les renseignements de santé à communiquer aux professionnels de la santé. Le caractère éphémère et circonscrit du « problème de santé ponctuel non urgent » milite en faveur d'un consentement d'une étendue limitée aussi bien dans le temps (le temps d'une consultation) que dans l'espace (un professionnel à la fois) et dans le contenu (état de santé actuel).

Épisodes de soins

L'usager peut aussi être aux prises avec des problèmes de santé particuliers qui nécessitent une *intensité de soins* dans un *continuum de services* dispensés par *différents professionnels*, en *divers lieux*, pendant une *période donnée*. L'usager entre alors dans ce qu'il est convenu d'appeler un épisode de soins[59]. Or, le virage ambulatoire fait en sorte que l'épisode de soins et autres traitements de courte durée se déroulent de moins en moins à l'hôpital et de plus en plus dans la communauté. Nous sommes conscients que le

[59] La Régie régionale de la santé et des services sociaux de Laval définit l'épisode de soins « comme étant la séquence complète des actions qui doivent être réalisées pour atteindre l'objectif du traitement en courte durée d'une condition clinique donnée pour un usager » (2001 : 3).

succès du virage ambulatoire repose sur des moyens technologiques et organisationnels qui favorisent la communication des renseignements cliniques entre les professionnels de la santé oeuvrant dans différents lieux de dispensation. Nous reconnaissons aussi qu'il peut être difficile d'obtenir le consentement manifeste de l'usager chaque fois qu'un professionnel met à jour ou visualise à distance un dossier propre à un épisode de soins. Dans ce cas-ci, le consentement nous apparaît raisonnable dans la mesure où il peut se limiter à la durée de l'épisode de soins (limite temporelle) et à des professionnels qui dispensent des soins à l'usager en fonction de profils de pratique donnée (limite spatiale) à l'intérieur de cet épisode.

Situations d'urgence

Les situations d'urgence sont souvent évoquées pour souligner les limites d'un consentement éclairé au moment de l'utilisation de l'inforoute par les professionnels de la santé. La communication de l'information en situation d'urgence doit se faire rapidement et être ciblée. De plus, l'usager peut être confus ou inconscient. Dans ces conditions, il peut être impossible pour l'usager d'exprimer un consentement éclairé au moment de l'intervention de l'équipe soignante. Cette incapacité de l'usager à exprimer un consentement valide ne devrait pas empêcher les professionnels de la santé à accéder aux renseignements cliniques nécessaires, où qu'ils soient. Ceci dit, nous considérons qu'il est important que ce même usager exerce, ici aussi, un certain contrôle sur la communication de ses renseignements. Ce contrôle peut s'exercer *a priori*, en permettant à l'usager d'autoriser au préalable la communication de certains renseignements jugés nécessaires à des professionnels de la santé en situation d'urgence dans un contexte d'inforoute. Le contrôle de l'usager pourrait aussi s'exercer *a posteriori*, en lui permettant d'accéder à la liste des intervenants qui ont visualisé ou mis à jour les renseignements de santé réseautés qui le concernent.

Comme le montrent ces exemples, le consentement peut être plus ou moins étendu dans le temps, dans l'espace et dans le contenu selon les situations cliniques qui prévalent, comme il peut s'exprimer en temps réel, au moment de la communication des renseignements de santé, ou *a priori*, avant même de rencontrer les professionnels de la santé. Il peut être aussi plus ou moins explicite selon la sensibilité et la nécessité clinique des renseignements disponibles. En somme, il semble important, dans un contexte d'inforoute, de ne pas voir le consentement comme un processus rigide et fixe, mais

plutôt comme une mécanique que l'on doit moduler en fonction de situations cliniques particulières tout en favorisant un consentement limité dans le temps, dans l'espace et dans le contenu. En principe, quelle que soit la mécanique retenue, l'usager devrait pouvoir s'affranchir de son passé, surtout quand celui-ci a perdu sa nécessité clinique. De la même façon, il devrait pouvoir continuer à garder certains secrets, particulièrement lorsqu'il s'agit de renseignements jugés socialement sensibles. Ceci dit, il y a lieu de pousser plus loin la réflexion sur la mécanique du consentement et d'expérimenter les formes qu'elle peut prendre dans le cadre de l'inforoute.

5. ÉLÉMENTS DE RÉFLEXION À APPROFONDIR

En guise de conclusion et à la lumière de ce qui précède, il convient de revenir sur ce qui nous apparaît être des questions essentielles auxquelles il faut apporter des réponses avant d'aller plus loin dans le déploiement d'une inforoute de la santé au Québec. Ces questions peuvent être regroupées sous les deux thèmes suivants :

1) Centralisation des renseignements de santé et création de nouveaux dossiers cliniques

Une des tendances que fait apparaître la présente analyse des projets de mise en réseau des dossiers est la création de nouveaux dossiers informatisés qui tendent à centraliser les renseignements cliniques sur une base régionale ou nationale. Or, les risques liés la création et à la mise en réseau de ces entrepôts de données cliniques sont considérables. Avant d'aller de l'avant, il est nécessaire d'en justifier la nécessité. Y retrouvera-t-on l'ensemble des renseignements cliniques de la population d'une région, voire du Québec? Qui pourra y accéder? Quel usage pourra en faire le gouvernement pour des raisons d'intérêt public? L'intérêt public ou les besoins de la science auront-ils préséance sur le droit à la vie privée? Le médecin aura-t-il accès à tout le contenu? Dans quelle mesure et selon quelles conditions les chercheurs pourront-ils utiliser ce contenu sur une base nominative? Comment s'exprimera concrètement le consentement de l'usager de ce contenu quant à la communication à des tiers? Doit-on éviter dans la mesure du possible la constitution de dossiers cliniques centralisés permanents qui se superposeraient aux dossiers locaux existants?

2) Détenteur légal et gardien des renseignements cliniques

Dans un contexte de centralisation des renseignements cliniques sur une base régionale ou nationale, qui deviendra le détenteur juridique et le gardien physique de ces renseignements? Qui assurera la sécurité de ces informations et le respect des règles de confidentialité? S'agira-t-il d'une responsabilité partagée? À qui devra s'adresser la personne qui voudra avoir accès à son dossier ou formuler une demande de rectification de renseignements qui seront inexacts, incomplets ou équivoques? Quelles règles juridiques encadreront l'utilisation et la communication de ces renseignements? Plus globalement, doit-on prévenir la concentration à l'intérieur d'organismes de renseignements de santé qui ne seront pas nécessaires à l'exercice de leurs attributions

et de leur mission ou à la mise en œuvre d'un de leurs programmes dont ils ont la gestion?

CONCLUSION

Cette étude permet d'illustrer que plusieurs modèles d'architecture de dossiers cliniques informatisés existent au Québec et que chacun de ces modèles est porteur de mécanismes d'accès, de consentement et d'entreposage de données. Or, ces modèles sont souvent à la remorque d'une technologie précise ou d'un projet particulier, lequel détermine les modes d'usage de l'information clinique et les principes qui les sous-tendent.

Au regard des tendances qui caractérisent le déploiement de l'inforoute de la santé, une question préoccupe particulièrement la Commission : pour quelle raison l'information clinique doit-elle être dupliquée systématiquement et entreposée dans des banques centrales? Autrement dit, pourquoi l'information clinique ne serait-elle pas accessible là où elle se trouve localement, plutôt que d'être centralisée régionalement ou nationalement?

Par ailleurs, la Commission réitère la nécessité de revoir le cadre juridique québécois concernant la protection des renseignements de santé à la lumière des nouvelles dynamiques d'échanges d'information clinique utilisée dans l'intérêt du patient. La révision du cadre juridique doit être à la fois globale dans sa portée et neutre au plan technologique.

Enfin, la Commission est consciente que la constitution de dossiers cliniques informatisés et leur mise en réseau représentent une ressource stratégique non seulement pour l'équipe soignante, mais aussi pour différents agents de la société, tels les planificateurs, les chercheurs et les entreprises, tant dans le secteur public que privé. Que l'on pense à des finalités administratives pour assurer la gestion courante des programmes de santé, à des finalités épidémiologiques dans l'optique d'améliorer la santé publique, à des finalités scientifiques dans une perspective de recherche ou à des finalités économiques qui s'appuient sur la commercialisation des renseignements cliniques et des systèmes technologiques déployés. Or, on se doit d'être vigilant quant à un possible élargissement des finalités du dossier clinique informatisé et à ses conséquences sur la protection de la vie privée. D'importantes réflexions et débats

restent à faire avant d'étendre l'utilisation du dossier clinique informatisé à d'autres finalités que celle qui vise à poser un diagnostic ou à traiter un patient.

BIBLIOGRAPHIE

Anderson, J.G. (2000), Security of the Distributed Electronic Patient Record : a Case-Based Approach to Identifying Policy Issues, *International Journal of Medical Informatics*, 60: 111-118.

Breton, Brigitte, *Le Soleil* du 2 mai 2001, Le bon usage d'une carte.

Collège des médecins, mémoire déposé au Colloque sur les orientations stratégiques du MSSS, juin 2000.

Dutrisac, Robert, *Le Devoir* du 30 avril 2001, Vers un relevé individuel du coût des soins de santé. Trudel fait miroiter tous les bénéfices d'une carte à puce.

France Presse, *La presse*, jeudi 21 décembre 2000, De nouvelles règles pour protéger les informations médicales privées.

Fernet, Paul, présentation lors du colloque sur *L'informatisation des dossiers de santé : enjeux de droits, enjeux de société*, 9 mai 2001.

Health Privacy Project, New Regualtion Restricts Employer Access to Health Information and Gives patients New Rights, site Internet : www.healthprivacy.org.

Jennifer Stoddart, présidente de la Commission d'accès à l'information, allocution prononcée lors du colloque sur *L'informatisation des dossiers de santé : enjeux de droits, enjeux de société*, 9 mai 2001 à Montréal.

Ministère de la Santé et de Services sociaux, (2001), *Les orientations technologiques du réseau sociosanitaire : Pour un accès intégré et sécurisé à l'information*, Document synythèse.

Péladeau, Pierrot, *Le Devoir* du 2 mai 2001, Carte santé à microprocesseur : l'incontournable débat public.

Pendrack, R.F. et R.P. Ericson (1998), Information Technologies Need to Protect Patient Confidentiality, *Health Financial Management.*

RAMQ (1996), *Évaluation du projet d'expérimentation de la carte santé à microprocesseur. Version abrégée du rapport final* : 18.

RAMQ, *Procédures d'accès au système de carte santé à microprocesseur. Projet Vitrine PRSA-Carte Santé – Volet Pharmacie.*

Régie régionale de la santé et des services sociaux de Laval, Document de positionnement de la sécurité du SI-PRSA, Projet Vitrine PRSA – Carte santé, 13 mars 2001.

Safran, C et H. Golberg (2000), Electronic Patient Records and the Impact of the Internet, *International Journal of Medical Informatics,* 60 : 77-83.

SOGIQUE, *Rapport synthèse de l'analyse préliminaire du projet dossier patient partageable* présenté par Réginald Blanchard au colloque de l'AHQ le 23 novembre 2000 : 8

Trudel, Rémy (2001), mémoire déposé au Conseil des Ministres, *L'implantation de la Carte d'accès Santé à microprocesseur et la contribution de la RAMQ à la modernisation du système de Santé et des Services sociaux*.

Turenne, François, allocution prononcée au Salon annuel *Informatique-Santé* de l'AHQ, 22 novembre 2000.

Vérificateur général du Québec, Rapport annuel 1999-2000

Washington Post du 15 février 1998, cahier A1, Prescription Sales Privacy Fears.

#

ANNEXE I

SURVOL RAPIDE DES RÈGLES AMÉRICAINES CONCERNANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE CADRE DU HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Jusqu'à tout récemment, aux États-Unis, l'accès et la protection des renseignements personnels dans le secteur de la santé étaient assujettis à des lois disparates qui variaient d'un État à un autre. De façon générale, les lois adoptées par les différents États américains, tout comme le « Privacy Act » adopté par le gouvernement fédéral en 1974, ne couvrent pas les usages secondaires des renseignements de santé par des organisations privées, notamment à des fins de commercialisation[60] ou d'embauche[61].

> Par un simple clic sur la souris, et sans votre consentement, les informations personnelles sur votre santé sont accessibles à des gens que vous ne connaissez pas, qui ne sont pas médecins, pour des raisons qui n'ont rien à voir avec vos soins[62].

La dénonciation et prise de conscience de ces pratiques quasi institutionnalisées incitent de plus en plus d'américains à cacher de l'information de santé ou à la maquiller.

> One out of every six people engages in some form of privacy-protective behaviour to shield themselves from the misuse of their health information, including withholding information, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and – in the worst cases – avoiding care altogether[63].

Afin que cessent les pratiques douteuses quant à l'utilisation secondaire des renseignements de santé et pour rassurer une population américaine de plus en plus inquiète pour sa vie privée, le Président Clinton fait approuver par le Congrès, en 1996,

---

[60] L'industrie du forage des données [data mining] est aux États-Unis une industrie lucrative qui génère annuellement environ 10 milliards de revenu (Anderson, 2000). Par ailleurs, comme le soulignait le Washington Post (1998), de nombreuses chaînes de pharmacies américaines vendent aux fabricants pharmaceutiques des profils de consommation et de prescription des médicaments.

[61] Selon une étude menée auprès des 500 plus grosses entreprises américaines, le tiers de celles-ci ont eu recours à des renseignements de santé dans leurs décisions d'embauche (Pendrak et Ericson, 1998)

[62] Traduction des propos du président Clinton rapportés dans *La presse* du jeudi 21 décembre 2000, De nouvelles règles pour protéger les informations médicales privées, France Presse.

une loi fédérale, le Health Insurance Portability and Accountability Act [ci-après HIPAA] qui, contrairement au Privacy Act, couvre non seulement les organisations de santé du secteur public, mais aussi celles du secteur privé.

Par l'adoption de cette loi, le gouvernement américain entend également normaliser, pour des raisons d'efficience et d'économie[64], les transactions financières et administratives entre les dispensateurs de soins, les assureurs et les entreprises [clearinghouse[65]] qui traitent et acheminent l'information entre les deux précédentes organisations. Deux importantes mesures de normalisation sont envisagées : d'une part, imposer un numéro unique aux usagers, aux dispensateurs de soins, aux assureurs et autres organisations directement engagées dans la dispensation des soins et des services de santé[66] et, d'autre part, forcer l'utilisation de systèmes de codification [standard code sets] qui permettront d'échanger aussi bien des données cliniques (CIM9, ICD-9, HL7) que des données financières (CPT).

Après une large consultation publique au cours de laquelle plus de 50 000 commentaires ou mémoires [comments] furent recueillis, la plupart provenant de citoyens ou de représentants de la population, le Département de Santé américain [Health and Human Services Department] publie une version détaillée des règles légales qui régiront la protection des renseignements de santé personnels. Malgré une vive opposition de l'industrie de la santé, mais fort de l'appui de la population et de ses représentants, HIPAA entre en vigueur le 14 mai 2001, quelques mois après l'arrivée au pouvoir du Président Bush. Les organisations du secteur de la santé visées par cette loi ont deux ans pour s'y conformer. Il s'agit d'une loi plancher qui a préséance sur les lois existantes moins sévères promulguées par les États américains. Quant aux lois américaines qui offrent des garanties de protection de l'information de santé plus strictes, elles continueront à s'appliquer.

---

[63] Health Privacy Project, New Regulation Restricts Employer Access to Health Information and Gives patients New Rights, site Internet : www.healthprivacy.org.

[64] Le gouvernement américain estime les coûts d'implantation sur 10 ans à 17.6 milliards en dollars américains et les économies à 29.9 milliards de dollars.

[65] Selon l'article 160.103 (HIPAA), « *Health care clearinghouse* means a public or private entity, including a billing service, repricing company, community health management information system or community health information, and "valued-added" network and switches. »

[66] La création d'un identifiant unique pour les usagers rencontre d'importance résistance aux États-Unis. Ses détracteurs craignent voir l'État ou l'entreprise privée se doter d'un mécanisme lui permettant d'accéder à tous les dossiers de santé des citoyens. Le gouvernement américain semble avoir mis sur la glace cette mesure.

Par rapport à la situation actuelle, HIPAA donne aux consommateurs plus de contrôle sur leurs renseignements de santé afin d'éviter la diffusion et la vente de ceux-ci à des organisations non autorisées. Lorsque cette loi sera implantée dans deux ans, les intervenants de la santé et les organisations dans lesquelles ils œuvrent devront demander à l'usager une autorisation écrite avant d'utiliser à l'interne ou de divulguer à l'externe leurs renseignements de santé dans le cadre d'activités courantes, comme entreprendre un traitement, évaluer l'acte clinique, faire de l'enseignement ou procéder à des opérations de paiement.

Cette autorisation comprendra une notice indiquant à l'usager 1) comment les renseignements le concernant seront utilisés à l'interne et divulgués à l'externe, 2) comment il pourra accéder à ses propres renseignements, cliniques ou administratifs, et 3) quelles seront les organisations qui accéderont ou pourront accéder aux renseignements de santé le concernant sans son consentement et quelles seront les raisons de cette communication sans autorisation[67].

De plus, une autorisation écrite distincte devra être obtenue auprès de l'usager avant de communiquer des renseignements de santé le concernant à des organisations qui n'offrent pas directement de soins ou de services de santé à l'usager, à savoir les entreprises financières, les fabricants de médicaments, les entreprises de (télé)marketing et la majorité des employeurs. Une autorisation explicite distincte est aussi requise avant de divulguer les notes psychothérapeutiques d'un usager à un tiers.

À sa demande, l'usager aura accès à ses dossiers cliniques et aux données financières le concernant. Il pourra alors exiger des corrections si l'information est erronée. Il pourra aussi connaître la liste de toutes les organisations ou personnes qui ont consulté durant les six dernières années ses dossiers en dehors d'opérations de routine, que sont le traitement clinique et le paiement ou remboursement des services, ainsi que les raisons de ces consultations et l'information consultée.

---

[67] Une organisation peut communiquer à une autre les renseignements de santé d'un individu sans son consentement dans le cadre de la santé publique, de procédures judiciaires, d'interventions en situation d'urgence, de menaces à la vie de personnes, d'identification du corps d'une personne décédée, d'activités de défense et de sécurité nationale, de barrières de communication.

La loi s'applique à tous les renseignements de santé utilisés ou divulgués par les organisations visées, peu importe le format utilisé : électronique, papier ou parole. Les personnes qui contreviennent à HIPAA, en divulguant des renseignements personnels à des fins commerciales sans le consentement des usagers concernés, peuvent être passibles jusqu'à 10 ans de prison et d'une amende pouvant atteindre 250 000 $ dollars américains.

Alors qu'HIPAA reçoit l'appui de plusieurs groupes de consommateurs et autres représentants de la population, l'industrie de la santé[68] conteste cette loi en soutenant que les coûts dépasseront les économies et qu'il est irréaliste d'exiger un consentement explicite pour chaque utilisation ou communication de renseignements personnels. L'Association médicale américaine, quant à elle, dénonce le laxisme en ce qui concerne l'accès par les appareils administratifs de l'État, en particulier le HHS, aux renseignements de santé personnels. Enfin, les pharmaciens s'opposent au fait qu'ils ne pourront plus délivrer les médicaments prescrits par téléphone. Le HHS se donne la première année pour apporter les modifications qui faciliteront l'implantation d'HIPAA.

[68] en particulier les associations d'hôpitaux, dont l'American Hospital Association (AHA), des HMO, des assureurs privés et des fabricants pharmaceutiques. Par exemple, selon l'AMA, les usagers auront à signer un document d'autorisation d'une longueur pouvant dépasser dix pages avant de permettre l'utilisation ou la communication de leurs renseignements personnels.

ANNEXE II

SURVOL RAPIDE DES RÈGLES EUROPÉENNES CONCERNANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE CADRE DE LA DIRECTIVE EUROPÉENE

Toutes les règles internationales reprennent les grands principes reconnus en matière de protection des renseignements personnels (fair information practices) et également édictées par les législations nationales. Les plus importantes de ces règles peuvent se résumer comme suit :

- seuls doivent être recueillis les renseignements nécessaires aux fins poursuivies, par des moyens licites et, le cas échéant, après en avoir informé la personne;
- les données recueillies doivent être exactes, complètes et tenues à jour;
- les données ne devraient pas être utilisées à des fins autres que celles pour lesquelles elles ont été recueillies et elles ne devraient pas être communiquées à des tiers à moins que la personne concernée n'y ait consenti ou qu'une règle de droit ne le prévoit;
- les données doivent être conservées de façon sécuritaire;
- les organismes qui traitent des données doivent le faire de façon transparente;
- les données doivent être accessibles aux personnes concernées;
- une personne peut exiger la rectification des renseignements qui seraient inexacts ou incomplets à son sujet.

Directive Européenne 95/46/CE[69]

Cette Directive européenne, que doivent obligatoirement respecter les États membres, est sans contredit le texte le plus important en matière de protection des données personnelles dans le cadre de la législation communautaire européenne.

L'objet de cette directive, adoptée le 24 octobre 1995, vise l'atteinte de deux objectifs à première vue irréconciliables. Premièrement, la Directive oblige les membres de l'Union européenne à assurer la protection des libertés et droits fondamentaux des personnes physiques notamment dans leur vie privée, à l'égard du traitement des

données à caractère personnel. Deuxièmement, la Directive édicte aux États membres de ne pas restreindre la libre circulation des données à caractère personnel entre eux si les obligations décrites ci-dessus sont respectées.

Le traitement des données à caractère personnel réfère à la cueillette, le conservation, l'utilisation et la communication des renseignements.

Conformément à l'article 8 de cette Directive, les États membres doivent interdire le traitement de données généralement qualifiées de sensibles : renseignements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Pour déroger à cette règle, la personne concernée doit y consentir sauf si l'État membre a prévu des situations où même le consentement de la personne concernée ne peut lever l'interdit de traitement des données personnelles (situation où l'intérêt public ne permet aucun traitement des données sensibles).

D'autres exceptions au principe général énoncé par l'article 8 sont prévues par cette même disposition. Ainsi, le traitement des informations à caractère sensible est possible dans les situations suivantes :

- la législation nationale peut lever l'interdit en matière de relations de travail dans la mesure où des garanties adéquates protègent les renseignements;
- le traitement de l'information vise la défense d'intérêts vitaux d'une personne dans l'incapacité de consentir;
- le traitement est fait par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale si les données concernent les membres de l'organisme et qu'il s'agit d'un traitement effectué dans le cadre d'activités légitimes. Dans ce cas, des garanties appropriées doivent être prévues par l'organisme et la communication de renseignements à des tiers ne peut se faire sans le consentement de la personne concernée;

---

[69] Directive 95/46/CE du Parlement Européen et du Conseil relative à la Protection des Personnes Physiques à l'Égard du Traitement des Données à Caractère Personnel et à la Libre Circulation de ces Données

- la personne a elle-même rendu ces informations publiques ou ces dernières sont nécessaires à des fins de justice;
- le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de la gestion des services de santé et que le traitement est effectué par un praticien de la santé régit par le secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente;
- la législation d'un État membre ou une décision de l'autorité de contrôle peuvent, si des garanties appropriées sont prévues, prévoir d'autres règles d'exception si un motif d'intérêt public important le prévoit.

La Directive européenne prévoit donc les règles auxquelles doivent se soumettre les États membres en matière de protection des données personnelles, y compris les données personnelles relatives à la santé. Toutefois, seule une analyse des législations nationales peut permettre de dresser un portrait global de la situation.

L'article 25 de la Directive prévoit qu'un État membre ne peut communiquer de données personnelles à un État tiers si ce dernier n'a pas un niveau de protection adéquat. Cette disposition a donné lieu à toute une saga relative aux flux transfrontières de données entre les membres de l'Union européenne et les États-Unis. Une entente dite du havre de sécurité (safe harbor) a été conclue avec les États-Unis. Cette dernière entente s'applique peu importe la catégorie à laquelle appartient le renseignement personnel. L'entreprise américaine doit respecter dans les grandes lignes les principes de protection des renseignements personnels décrits au début de cette section. Par ailleurs, l'entreprise européenne doit offrir aux personnes concernées la possibilité de refuser la communication de renseignements la concernant (opt out). Toutefois, si cette communication concerne des renseignements sensibles, dont des renseignements relatifs à la santé, l'entreprise européenne doit obligatoirement obtenir le consentement de la personne concernée (opt in). Des exceptions sont cependant prévues à cette dernière règle. Ces exceptions sont à toutes fins pratiques identiques à celles prévues à l'article 8 de la Directive européenne.

L'Organisation de développement et de coopération économique a également adopté, en 1980, des lignes directrices en matière de protection des données et du flux transfrontière de données. Toutefois, ces lignes directrices ne sont pas obligatoires.

Les Nations Unies ont également, en 1990, adopté des lignes directrices relatives au traitement automatisé des données personnelles.