ÉVALUATION DU PROJET

VITRINE DOSSIER CARTE SANTÉ DE LAVAL

DE LA RÉGIE DE L'ASSURANCE MALADIE DU QUÉBEC

Décembre 2001

TABLE DES MATIÈRES

1. INTRODUCTION

Nous assistons actuellement à un accroissement du recours à de nouvelles technologies de la part des différentes administrations publiques, et ce, particulièrement dans le réseau de la santé. Différents projets pilotes sont réalisés pour juger de la faisabilité d'implanter ces technologies. Le projet vitrine dossier carte santé à Laval est de cette mouture. Or, les technologies de l'information et des communications, et, par extension, les applications qui en résultent, peuvent avoir des impacts potentiels sur la protection de la vie privée et des renseignements personnels des citoyens et des utilisateurs de ces technologies. À cet égard, notre examen du système dossier carte santé (DCS) met en relief les différents impacts de l'introduction de la technologie utilisée dans ce projet, soit un fichier réparti en partie dans une banque de données et en partie sur une carte à microprocesseur. Plus concrètement, après une brève présentation du système, nous décrivons le projet en cause et nous en apprécions divers aspects, tout en différenciant les spécificités propres à la carte intervenant et celles propres à la carte du patient.

Conformément au mandat qui lui a été reconnu par le législateur, et tel qu'elle s'y était engagée, la Commission d'accès à l'information (CAI) a donc mené une évaluation du projet vitrine carte santé. Ce projet, dont le maître d'oeuvre est la Régie de l'assurance maladie du Québec (RAMQ), s'est déroulé dans la région de Laval de 1999 à 2001. Toutefois, la RAMQ y a mis un terme plusieurs mois avant l'échéance prévue.

2. PORTÉE DE L'ÉVALUATION

La présente évaluation porte principalement sur les aspects conceptuels et juridiques du système DCS mis en place par la RAMQ.

La technologie de carte à microprocesseur, les applications, les télécommunications et les logiciels utilisés n'ont pas fait l'objet d'un audit.

Compte tenu du très faible nombre d'utilisateurs et du peu d'occasions où la carte pouvait être utilisée, le présent examen ne porte pas non plus sur les facteurs d'appréciation de la clientèle, contrairement à ce

que la CAI a fait lors de l'expérience de carte à microprocesseur menée dans la région de Rimouski de 1993 à 1995[1].

Les éléments qui soutiennent le présent rapport ont été recueillis par l'examen de documents et par le biais d'entrevues.

[1] Commission d'accès à l'information, *Avis relatif au projet pilote de carte santé à microprocesseur mené dans la région de Rimouski*, mars 1996, 43 p.

3. CARTES À MICROPROCESSEUR ET CARTES À MICROPROCESSEUR AVEC INDEX

Une carte à microprocesseur est une carte plastifiée au sein de laquelle est intégré un microprocesseur. Elle fonctionne grâce à diverses composantes contenues sur le microprocesseur, principalement un OS (Operating System) et de la mémoire. Sa particularité est sa capacité à effectuer des traitements à l'intérieur du microprocesseur de façon autonome. On accède généralement au contenu d'une carte par l'entremise d'un lecteur. Il existe des cartes avec contacts qu'on doit insérer dans tel lecteur et d'autres sans contacts plutôt munies d'antennes radio.

La carte à microprocesseur est une technologie d'origine européenne; c'est donc sur ce continent qu'on trouve les principaux manufacturiers nommés *encarteurs*. Les plus connus d'entre eux sont : Gemplus, Schlumberger, De La Rue, Oberthur et Orga.

Les applications les plus répandues de la carte sont : porte-monnaie électronique, programmes de fidélité, applications bancaires, commerce électronique et applications basées sur les infrastructures à clés publiques. L'intérêt d'utiliser la technologie de la carte à microprocesseur est précisément la possibilité nouvelle de décentraliser les données et les traitements dans une technologie portable.

Les cartes à microprocesseur possèdent une mémoire limitée, ce qui exclut la possibilité d'emmagasiner une grande quantité de données. C'est pour répondre à cette limitation qu'a été créée la carte avec pointeurs. Cette technologie permet d'entreposer de l'information dans des banques de données ou des fichiers externes à la carte. Ainsi, certaines données continuent de résider sur la carte, mais la plupart de celles-ci sont emmagasinées ailleurs. Rappelons que la carte à microprocesseur est une technologie qu'on intègre à un système. La carte en soi n'est qu'un élément de ce système d'information qui doit être considéré dans son ensemble.

4. RISQUES LIÉS À LA TECHNOLOGIE

Les risques et les failles de sécurité concernant la carte à microprocesseur sont peu diffusés. Les attaques les plus répandues sont celles concernant les cartes bancaires et les cartes à microprocesseur autorisant l'accès satellitaire à des chaînes de télévision payante.

Les experts français font état de deux grands types d'attaques dont les cartes peuvent faire l'objet. Le premier type implique des modifications du microprocesseur par des procédés chimiques, optiques ou autres. De telles modifications demandent des équipements spécialisés et certaines connaissances techniques. L'autre type d'attaques laisse le microprocesseur intact et profite des vulnérabilités logicielles. Citons par exemple les vulnérabilités des OS, des interfaces de communications, des protocoles et des algorithmes cryptographiques.

Le gouvernement français désireux d'augmenter la confiance des citoyens envers cette technologie a décidé de procéder à l'évaluation de la sécurité de celle-ci. Cette tâche est confiée à des organismes indépendants, objectifs et impartiaux nommés Centres d'évaluation de la sécurité des systèmes d'information (CESTI). Les normes d'évaluation étant reconnues internationalement, des organismes équivalents existent aujourd'hui partout dans le monde, y compris au Canada.

> « *Toutes ces attaques ont pour but la divulgation ou la modification d'informations sensibles, par exemple un numéro d'identification personnelle, des clés cryptographiques ou des fichiers de données.* »[2]

L'utilisation d'une carte avec pointeurs ou d'un modèle de carte utilisant une mémoire externe induit des risques supplémentaires potentiels qu'une évaluation de sécurité menée selon des normes internationales reconnues permettrait de répertorier complètement.

[2] Site du Premier ministre de la République française - Augmenter la confiance - L'évaluation des cartes à puces (www.scssi.gouv.fr/fr/confiance/cartes.html).

5. RIMOUSKI ET LAVAL : UNE DISTINCTION S'IMPOSE

La CAI a émis des commentaires sur le projet d'expérimentation de carte à microprocesseur tenu à Rimouski de 1993 à 1995. Ce projet offrait au patient un aide-mémoire informatisé que celui-ci transportait avec lui et pouvait présenter lorsqu'il consultait un professionnel de la santé. Le patient en contrôlait la mise à jour, la consultation et il en était l'unique gardien.

L'architecture du système DCS utilisé à Laval est différente. Si, comme à Rimouski, des données résident sur la carte, d'autres résident dans une banque de données centrale détenue à la RAMQ.

Cette distinction fondamentale entre les deux projets doit être rappelée. Vouloir transposer au projet de Laval les commentaires formulés par la CAI dans son avis de 1996 est donc tout à fait inapproprié.

6. DESCRIPTION DU SYSTÈME DCS

Historique

Au printemps 1998, la RAMQ fut mandatée par le gouvernement pour démontrer certains aspects fonctionnels du système d'information DCS dans le cadre du projet système d'information - programmation régionale des soins ambulatoires (SI-PRSA), à Laval.

Le décret 1177-99 consacre ce mandat. Le décret énonce les obligations de la RAMQ dont la suivante : *«... à démontrer... les principales fonctionnalités et à exposer certains concepts entourant le volet clinique du système de carte santé à microprocesseur, soit : l'utilisation de carte à microprocesseur et d'une banque de données anonymes pour l'accès et la sécurisation du dossier carte santé et la gestion du consentement de l'usager à l'accès à son dossier carte santé...* ». Il est de plus précisé : « *En aucun temps, elle (la RAMQ) ne peut avoir accès au contenu de la banque de données anonymes. Elle doit cependant s'assurer de la gestion du système, des différents éléments de sécurité, du succès des transactions et de la disponibilité du système.* ». Le libellé du décret se termine comme suit : « *Qu'à la suite de la réalisation du projet vitrine PRSA-Carte santé, un débat public sur les enjeux sociaux, éthiques et juridiques du projet de la carte santé à microprocesseur soit tenu préalablement à la décision de l'implantation du système à l'échelle du Québec* ».

Le projet vitrine PRSA-Carte santé a été inscrit par le gouvernement du Québec comme participant au projet Netlink. Ce projet lancé par la Commission européenne implique des participants de France, d'Allemagne et d'Italie. Son objectif est de définir des recommandations et de proposer des spécifications techniques pour permettre l'interopérabilité des systèmes d'information de carte santé. L'objectif de cette interopérabilité internationale est de permettre l'accès à certaines informations contenues sur la carte à partir de n'importe quel système à carte santé dans tous les pays participants.

Le projet de Laval devait s'étendre de janvier 1999 à mai 2002. Cependant, au printemps 2001, on annonçait le déploiement d'une carte à microprocesseur à l'échelle du Québec et, en septembre 2001, le ministre de la Santé et des Services sociaux mettait fin prématurément à l'expérimentation de Laval. Selon des données fournies par la RAMQ,

en mai 2001, 1 715 cartes destinées aux patients étaient émises dont seulement 304 étaient activées.

Trois volets de l'expérimentation

Le projet comprend trois volets : SI-PRSA, clinique privée et pharmacie. Initialement, un autre volet devait être implanté; il s'agit de l'accès au DCS par les ambulanciers.

- Volet SI-PRSA

Les cartes à microprocesseur sont utilisées en établissement[3] au sein du projet SI-PRSA. L'accès au SI-PRSA était contrôlé par l'utilisation de cartes intervenants jusqu'au 10 septembre dernier. Quant aux cartes des patients, elles permettaient au patient de verser le contenu du dossier PRSA ou une partie de celui-ci dans le DCS. Les télécommunications se font par le réseau RTSS. Le SI-PRSA fait l'objet d'une évaluation indépendante du DCS par la CAI.

- Volet clinique médicale

Une seule clinique privée a participé au projet : le Centre médical Laval. Cette clinique est un centre spécialisé en obstétrique, pédiatrie et gériatrie. On y compte 14 médecins et 11 secrétaires. Pour le besoin de l'expérimentation, l'application locale de gestion des dossiers cliniques a été adaptée afin de permettre l'accès et l'alimentation du DCS. Toutes les données échangées avec la RAMQ circulent sur un lien web sécurisé de Vidéotron.

- Volet pharmacie

La pharmacie Daniel Pilon réside dans des locaux attenants à la Clinique médicale Laval. Afin de permettre à cette pharmacie l'utilisation du DCS, elle a été reliée au réseau local de la clinique

[3] Cité de la Santé, CHARL, Hôpital juif de réadaptation, CLSC des Milles-Îles, CLSC Ste-Rose de Laval, CLSC du Ruisseau Papineau, CLSC du Marigot.

médicale. Ceci permet à la pharmacie de disposer du lien Vidéotron de la clinique pour communiquer avec la RAMQ.

Pour les besoins de l'expérimentation, le logiciel de gestion de dossiers locaux a été adapté afin d'interfacer avec le DCS.

La gestion des cartes à microprocesseur

Dans ce projet, des cartes sont distribuées à la fois à des intervenants et à des patients. L'émission et la gestion de ces cartes relèvent de la RAMQ, mais la gestion du système de cartes est décentralisée dans les établissements participants.

Les procédures d'émission de cartes à microprocesseur sont indépendantes de l'émission des cartes d'assurance maladie. Aucune validation n'est effectuée au fichier d'inscription des personnes assurées et aucune validation n'est effectuée au fichier d'inscription des professionnels (de la santé).

La gestion des cartes s'effectue par le biais des logiciels VigiCarte et VigiMaître développés par la firme Motus Technologies inc. (Motus). VigiMaître est présent sur tous les postes utilisés dans l'expérimentation et sur lesquels sont branchés les lecteurs de cartes.

En tout, six types de cartes sont émises et celles-ci ont toutes un délai de validité, c'est-à-dire une date de début et une date de fin[4].

La carte intervenant

Dans le projet, une carte d'habilitation est fournie à chaque intervenant, laquelle est obligatoire pour accéder aux systèmes. La carte intervenant jumelée au numéro d'identification personnelle (NIP) est le moyen d'authentification qui permet d'accéder au système DCS et un mécanisme de contrôle d'accès additionnel au système SI-PRSA. Cette carte procure l'accès à un système qui permet la consultation et l'alimentation du fichier DCS.

[4] Les types de cartes : usager, intervenant, temporaire (pour intervenant), administrateur local, administrateur central et administrateur de système.

Lors du démarrage du projet, tous les établissements impliqués ont fourni à la RAMQ l'identification de l'ensemble des intervenants participant au projet vitrine en y associant un profil. C'est grâce à cette liste que les cartes ont été initialement émises. Par la suite, les établissements PRSA transmettent les demandes par l'entremise du CHARL qui devient l'unique interloculeur de la RAMQ pour l'émission de cartes. La clinique privée et la pharmacie, quant à elles, transigent directement avec la RAMQ.

La RAMQ délègue certaines fonctions à un administrateur local mandaté par chacun des sites de démonstration, notamment pour l'activation et la réactivation d'une carte intervenant, la définition des domaines d'utilisation des cartes intervenants et la gestion des cartes temporaires. C'est l'administrateur local qui prépare les cartes avant leur remise aux intervenants.

En clinique privée, deux administrateurs locaux assurent le support local. Compte tenu qu'un système de gestion ne pouvait être déployé à distance, il a été exceptionnellement décidé qu'une carte d'**administrateur central** soit laissée au centre médical sous clé et peut être utilisée par les administateurs locaux si une de leurs cartes devenait inutilisable. Cette carte ne permet toutefois pas d'émettre une nouvelle carte.

Comme les cartes intervenants sont les clés d'accès au système DCS, des mesures de relève se devaient d'être mises en place afin de pallier aux oublis ou aux pertes de cartes. Aussi, dans chaque établissement, des cartes temporaires d'intervenants de chaque profil d'accès sont disponibles aux administrateurs. Si un intervenant oublie ou perd sa carte, celle-ci est désactivée et ses profils d'accès et son identification sont transférés sur la carte temporaire. Lorsqu'il la retrouve ou en reçoit une nouvelle, on désactive la carte temporaire et réactive sa carte régulière.

La carte usager (carte du patient)

Une carte destinée au patient est émise, sur une base volontaire, aux patients fréquentant un des sites de l'expérimentation. L'authentification de celui-ci est réalisée par la présentation de la carte

d'assurance maladie. L'intervenant conserve dans ses dossiers locaux une trace de la réponse du patient (a reçu l'information et accepté, a reçu l'information et refusé…). Les données nécessaires à l'émission de la carte sont extraites du dossier local et sont expédiées à la RAMQ. La pharmacie n'effectue pas de demande d'émission.

Le patient qui reçoit une carte est dès lors doté d'un DCS entreposé à la RAMQ qui pourra être alimenté et partagé, avec son consentement, grâce au système appartenant à la RAMQ. Lors de la réception de sa carte, le patient doit se présenter dans un établissement participant afin d'activer sa carte et d'y inscrire son NIP.

La carte du patient est indépendante de la carte d'assurance maladie de la RAMQ qui est toujours requise pour les fins administratives.

Consultation du DCS

Le patient, lors d'une consultation auprès d'un professionnel de la santé, présente à sa discrétion sa carte et compose son NIP pour autoriser celui-ci à accéder à son DCS. L'accès au DCS requiert aussi la présence d'une carte d'intervenant et ce dernier doit aussi composer son NIP.

La consultation du DCS peut s'effectuer par un module autonome de consultation ou par l'entremise des applications cliniques locales; toutefois, à ce moment, les données provenant du DCS sont identifiées spécifiquement.

L'affichage du DCS offre trois onglets. Initialement, c'est l'onglet *Informations d'urgence* qui s'affiche[5]. Les deux autres onglets disponibles sont : *Dossier et suivi médical*[6] et *Personnes à contacter et antécédents*[7].

[5] Les données sont : nom, prénom, sexe, date de naissance, langue, nom marital, pays d'origine, groupe sanguin, don d'organes, maximum 5 diagnostics d'urgence et dates avec possibilités de voir le détail, limite de 5 allergies (allergie, sévérité, confirmée, par, inscrit le).

[6] Tous les diagnostics, les types de suivi, les médicaments, les tests.

[7] Contacts professionnels, personnels, facteurs affectant la santé (exemple : habitudes de vie, orthèse prothèse…), les vaccins, les antécédents.

Aucune fonctionnalité n'a été développée pour que le patient consulte le contenu de sa carte de façon autonome, la présence d'un intervenant étant toujours requise.

Dans le projet d'origine, une interface devait permettre la consultation sans consentement en situation d'urgence. Cette fonctionnalité n'a pas été implantée.

Alimentation du DCS

L'alimentation exige que l'intervenant s'authentifie avec sa carte et son NIP et que le patient fasse de même.

L'intervenant saisit d'abord les données médicales au dossier clinique informatisé du patient (PRSA, Médicarte ou Mentor). Par la suite, l'alimentation du DCS est possible. Le patient a le choix d'accepter, de refuser ou d'annuler l'alimentation. S'il refuse, les données ne pourront plus être versées au DCS. S'il annule, les données demeurent disponibles pour alimentation ultérieure.

Dans le projet initial, il était prévu, lors de l'alimentation du DCS, que les éléments d'information pompés du dossier local vers le DCS puissent être visualisés par l'intervenant et le patient avant que le transfert d'information ne s'opère. En l'absence de cette interface, ni le patient, ni l'intervenant ne connaissent avec certitude les données versées au DCS.

Entreposage des données du système DCS

Le DCS est supporté à la fois par le microprocesseur de la carte et par une banque de données externe à la carte; cette banque est qualifiée d'anonyme par la RAMQ parce que les données d'identité résident sur le microprocesseur. La carte contient dans sa mémoire des pointeurs permettant de retrouver les données à la RAMQ. La carte à microprocesseur utilisée dans ce projet est une carte utilisant un index, ce qui permet d'entreposer physiquement un minimum de données sur la carte elle-même et autant de données que voulu à la RAMQ. Cette réalité est transparente à l'utilisateur.

De façon non exhaustive, le fichier entreposé à la RAMQ contient les informations sur les vaccins, les antécédents personnels et familiaux, les résultats de tests, les médicaments délivrés, le suivi médical, les diagnostics confirmés, les facteurs affectant la santé (conditions et habitudes de vie).

Le microprocesseur sur la carte, toujours de façon non exhaustive, contient les données systèmes[8], le NIP, une partie du dossier DCS, soit les données d'identification et les informations d'urgence (contacts, groupe sanguin, allergies, diagnostics).

Le système mis en place par la RAMQ nécessite la création de plusieurs fichiers en plus du DCS. Il s'agit principalement de la banque de données personnes, la banque de données tiers de confiance, le bottin des cartes et le fichier des clés. L'architecture prévoyait aussi une banque de données de sauvegarde qui n'a pas été implantée.

La RAMQ détient aussi les journaux[9] relatifs aux transactions d'émission et de gestion des cartes.

Initialement, toutes les transactions au DCS devaient être journalisées. À cause de contraintes techniques, seules les transactions au DCS faites par la clinique privée et la pharmacie sont l'objet d'une journalisation.

[8] Notamment le numéro de certificat, le numéro de clé de chiffrement, le type de carte (temporaire ou permanente), le type de porteur (usager, intervenant, administrateur).

[9] Relevé chronologique des transactions informatiques constituant un historique de l'utilisation des programmes, des systèmes ou des accès à des dépôts de données.

7. APPRÉCIATION DU SYSTÈME DCS

7.1 Appréciation générale

7.1.1 Objectifs du projet

Le projet de la RAMQ visait initialement l'expérimentation d'une technologie :

> « *Les principaux objectifs du programme relatif au projet vitrine PRSA-Carte santé, confié à la Régie, sont de démontrer les principaux mécanismes et d'exposer certains concepts, entourant le volet clinique du système de Carte santé pour l'accès, l'entreposage et la sécurisation des informations de même que la gestion du consentement de l'usager à l'accès à son Dossier Carte Santé.* »[10]

Pour le gouvernement, les objectifs poursuivis étaient aussi de nature technologique :

> « *ATTENDU QUE le projet vitrine PRSA - Carte santé permet de réaliser les objectifs… ceux du gouvernement du Québec d'assurer une visibilité au savoir-faire québécois en matière d'applications exploitant les cartes à microprocesseur et de participer sur le plan international à l'élaboration des normes, particulièrement dans les champs d'application des cartes santé.* »[11]

Or, pour mettre en œuvre le projet, d'autres objectifs de nature clinique furent énoncés :

> « *Les objectifs visés par le projet sont les suivants :*

[10] Décret du gouvernement du Québec, numéro 1177-99, 13 octobre 1999.
[11] Décret du gouvernement du Québec, numéro 1177-99, 13 octobre 1999.

- favoriser une meilleure continuité des soins et des services de santé;
- favoriser l'amélioration de la qualité des soins;
- démontrer la gestion du consentement de l'usager à l'accès à ses données cliniques;
- transmettre de façon sécurisée des renseignements cliniques;
- entreposer de façon sécurisée des données cliniques. »[12]

« *L'utilisation d'un « Dossier Carte Santé » contribue à favoriser une meilleure continuité des soins et des services de santé fournis à l'usager par un échange sécurisé d'informations cliniques entre les différents intervenants appelés à travailler dans le dossier de cet usager.*

Le projet doit également démontrer la gestion du consentement de l'usager à l'accès à ses données cliniques. Ces données doivent par ailleurs être transmises et entreposées de façon sécurisée. »[13]

Les conditions de réalisation du projet n'étaient pas favorables à l'atteinte de ces objectifs cliniques. En effet, le DCS, un modèle de dossier clinique partageable national, a été ajouté au modèle de dossier clinique partageable régional déjà en place dans le SI-PRSA. Le choix d'intégrer le DCS au SI-PRSA s'explique par le besoin du projet DCS de disposer d'un dossier médical électronique et le fait que la clientèle PRSA était déjà traitée en multi-établissements. Les patients qui acceptaient de participer au projet DCS possédaient dès lors deux dossiers partageables. Pour la clientèle PRSA, le dossier PRSA était suffisant pour permettre les échanges requis dans l'épisode de soins ambulatoires. Le DCS n'apportait rien de plus en matière d'échanges au niveau des soins rendus en établissement. Il est à noter que la majorité de la clientèle PRSA termine son épisode de soins à domicile et ne pouvait donc alimenter le DCS.

---

[12] Le système de la carte santé à microprocesseur - Guide de l'usager - Régie de l'assurance maladie du Québec (décembre 2000).

[13] Guide des fournisseurs - PROJET VITRINE PRSA - CARTE SANTÉ - Version 1.1 - Direction des orientations et du développement stratégique - Projet Vitrine PRSA - Carte santé.

Le projet DCS a été déployé auprès des établissements participants PRSA, mais aussi dans une clinique privée et une pharmacie. Le faible taux de pénétration du projet rend l'expérimentation du partage multi-établissements plus difficile.

Le dédoublement des dossiers partageables, la faible étendue du projet et le nombre peu élevé de cartes patients nous amènent à nous interroger sur l'apport clinique dont peut bénéficier un patient qui participe à l'expérimentation.

1. La Commission recommande que le promoteur d'une expérimentation technologique s'assure de ne pas induire par une expérience de nouveaux risques en matière de protection des renseignements personnels et d'offrir des garanties en terme de bénéfices cliniques pour les patients participants.

7.1.2 Cadre juridique

Le projet DCS vise la création d'un nouveau type de dossier médical, le dossier clinique partageable national, et donc un nouveau fichier central de renseignements personnels. Les dossiers cliniques locaux des dispensateurs de soins (établissement, clinique, pharmacie) demeurent et servent à alimenter ce dossier clinique national.

Ce nouveau type de dossier clinique n'est pas défini dans le cadre juridique actuel et soulève de nombreuses interrogations. Quelle est la nature du dossier clinique partageable? Comment justifie-t-on la constitution de ce nouveau fichier? À quels fins et usages est-il destiné? Ce fichier est-il requis pour l'accomplissement de la mission de l'organisme détenteur? La RAMQ peut-elle concilier son rôle d'assureur public et de gestionnaire de banques de données cliniques? Quel cadre juridique sera applicable à ce nouveau type de fichier de renseignements personnels?

Des interrogations demeurent quant à la finalité du DCS. Qu'est donc le DCS?

Le DCS : un sommaire sous le contrôle du patient

Le DCS, tel qu'expérimenté à Laval, peut être considéré comme un résumé clinique sous le contrôle du patient et dont la RAMQ n'est que le fiduciaire. Le DCS est effectivement un dossier que le patient accepte de constituer et dont il contrôle les moments d'alimentation et de consultation.

Le patient ne peut toutefois décider d'inscrire dans le DCS que le contenu entier d'une consultation et pas seulement une partie de celle-ci. Le sommaire ne peut être utilisé et complété par le patient directement; son médecin doit compléter le dossier clinique local et lui demander s'il accepte de verser cette information dans le DCS. C'est sans compter qu'il ne peut constater concrètement dans une consultation quelle information sera versée dans le DCS et qu'une fois inscrite, l'information ne peut être modifiée ou retirée par le patient. Initialement, ces deux éléments de contrôle de la part du patient devaient être intégrés au système.

De cette manière, si un patient ne souhaite plus partager, ne serait-ce qu'une seule information inscrite au DCS, son unique solution de repli est de cesser d'utiliser ce système.

Quel serait le contrôle effectif du patient sur son sommaire clinique, lorsque celui-ci est constitué selon des paramètres édictés par un tiers, à la suggestion de ce tiers et ensuite confié à ce même tiers?

Le DCS : un dossier soutenant les échanges de renseignements médicaux entre intervenants dans une continuité de soins

Un outil d'échanges de renseignements médicaux entre professionnels de la santé suppose que la pertinence du contenu échangé soit déterminée par ceux-ci. Par exemple, lorsqu'un patient est pris en charge par un autre établissement, la pertinence de l'information à communiquer est déterminée par un intervenant médical. La difficulté d'attribuer une finalité au DCS et le contrôle exercé par le patient sur l'alimentation rendent aléatoire pour un professionnel de la santé la pertinence de l'information contenue au fichier.

Alors, le DCS

Le DCS est un dossier clinique national partageable, volontaire, centralisé, permanent et détenu par la RAMQ. Les données contenues sur la carte et sur le DCS pour un individu ne forment qu'un seul et même dossier, et l'ensemble des cartes et des enregistrements du DCS ne forment qu'un seul et même fichier. La carte à microprocesseur et la répartition physique des données ne constituent dans ce cas qu'une mesure de sécurité.

L'objet du DCS est le partage ou la communication de renseignements cliniques entre les établissements et les autres entités du réseau de la santé. Or, la communication ne peut être considérée comme une fin en soi. Il faut comprendre que dans le cycle de vie d'un renseignement personnel, la communication se situe bien après la justification de la constitution d'un fichier de renseignements personnels, la nécessité de la collecte des informations et la détermination de la finalité et de l'utilisation.

Il ne fait aucun doute que l'absence d'un cadre juridique laisse planer de nombreuses questions relatives à tous les volets de l'introduction de la technologie des cartes santé à microprocesseur et d'un dossier patient partageable.

2. L'évaluation du projet DCS a permis de constater que le cadre juridique actuel ne prévoit pas l'existence de ce type de dossier. En conséquence, la CAI recommande que le statut juridique d'un nouveau dossier clinique partageable comme le DCS soit défini.

7.1.3 Deux types de cartes, un système

L'expérimentation de Laval impliquait l'émission de deux cartes à microprocesseur, la carte intervenant et la carte patient. La carte intervenant sert à des fins d'authentification de ce dernier lorsqu'il accède au système et la carte du patient permet l'interaction avec son dossier clinique. Ces deux cartes ont des finalités différentes et les systèmes les accueillant sont des systèmes distincts. Ceux-ci devraient donc gé-

nérer des fichiers de renseignements personnels distincts. C'est ainsi que notre appréciation portera d'abord sur le système d'habilitation professionnelle à l'origine de la carte intervenant et, ensuite, nous apprécierons le système DCS.

3. La CAI considère le système d'habilitation des intervenants et le système DCS comme des systèmes distincts même s'ils s'interfacent l'un avec l'autre, car leurs objectifs sont différents. Ces systèmes pourraient vivre indépendamment. Par exemple, la carte intervenant s'est intégrée au SI-PRSA comme mécanisme d'authentification sans que le dossier patient SI-PRSA ne soit géré par une carte à microprocesseur.

7.1.4 Respect des principes directeurs

Les principes directeurs que la RAMQ s'est donnée dans la présente expérimentation sont le respect de la vie privée et du secret professionnel, la transparence, le volontariat et l'exclusion de toute discrimination, le consentement libre et éclairé du patient, la clarté de l'information, la limitation de l'usage et de la divulgation des renseignements personnels, les droits d'accès et de rectification, les garanties de sécurité, les droits de recours auprès du Commissaire aux plaintes de la RAMQ et la responsabilité et l'imputabilité de la RAMQ quant à la sécurité de la banque de données anonymes (BDA).

Concernant la transparence et la clarté de l'information, nous croyons que la compréhension d'un patient sur l'intérêt d'un DCS à la RAMQ ne peut être réellement appréciée, puisque les finalités du DCS sont imprécises. De plus, dans l'alimentation du DCS, l'absence de l'interface de visualisation de l'information enlève beaucoup à la transparence.

Concernant l'exclusion de toute discrimination, la trace laissée dans le dossier local de la détention d'une carte par la personne est susceptible de porter atteinte à ce principe. En effet, cette cueillette de renseignements et son inscription dans le dossier local n'est pas indispensable et pourrait être à l'origine de pressions discriminatoires. Un médecin qui sait que le patient devant lui possède un DCS et ne lui permet pas de le

consulter pourra, sans nécessairement traiter le patient de façon discriminatoire, avoir l'impression que ce patient ne lui fait pas confiance.

Concernant la limitation de l'usage, la RAMQ garantit par ce principe que « *l'utilisation et la divulgation de renseignements contenus dans le Dossier Carte Santé de l'usager à des fins autres que la prestation de meilleurs services de santé, en raison d'une plus grande disponibilité de l'information, est interdite* ». L'utilisation des renseignements à d'autres fins demeure difficile à vérifier. La production du rapport en pharmacie d'une liste d'adresses des patients détenant une carte représente un exemple nous laissant croire que ce principe n'est pas respecté totalement.

Concernant le droit d'accès du patient au DCS, la présence des deux cartes est exigée et toute action doit obligatoirement se faire en présence d'un intervenant dans le cadre d'une consultation. Ainsi, le patient ne peut exercer son droit d'accès de façon indépendante comme à Rimouski où le Bureau carte santé offrait cette possibilité.

Quant au droit de rectification, il n'a pu être exercé dans l'expérimentation de Laval parce que la fonction d'alimentation des données du DCS ne peut qu'ajouter de l'information sans droit de rectifier le contenu. Comme le DCS était alimenté de façon volontaire, nous croyons que le patient aurait dû pouvoir faire retirer toute information à sa discrétion.

4. La CAI considère que des possibilités gratuites et indépendantes d'accès à l'information doivent être offertes aux citoyens afin qu'ils puissent exercer à leur discrétion leur droit d'accès et de rectification. La possibilité d'obtenir une copie papier du contenu de leur dossier devrait aussi être offerte lors de la création du dossier et à tout moment, sur demande, par la suite.

5. La possibilité de retirer toute information du DCS à la discrétion des citoyens doit être offerte.

7.2 Appréciation du système d'habilitation des intervenants

7.2.1 La gestion d'un système d'habilitation des intervenants

La carte intervenant est une avenue intéressante pour le contrôle d'accès aux renseignements cliniques et l'authentification des intervenants de la santé.

La RAMQ détient déjà un fichier des professionnels de la santé pour les fins de facturation. Toutefois, le fichage centralisé des professionnels et d'autres employés pour des fins d'authentification et de contrôle d'accès à des données cliniques locales, régionales ou nationales devrait faire l'objet d'une démonstration au plan de la nécessité. La constitution de ce nouveau fichier des intervenants, qui déborderait par ailleurs le bassin des professionnels qui facturent actuellement la RAMQ, devra être évalué à la lumière du cadre juridique en vigueur et de la mission de la RAMQ.

6. La CAI demande que soit justifiée la nécessité de constituer un fichier central de tous les intervenants pour les fins d'émission de la carte d'habilitation.

7.2.2 La gestion des cartes intervenants

Les cartes étant les clés d'accès au dossier médical pour les intervenants, la gestion de ces cartes est éminemment stratégique.

Le processus de gestion des cartes implique beaucoup d'acteurs; en plus de l'administrateur central qui est à la RAMQ, plusieurs administrateurs locaux sont requis aux fins de cette gestion. Ce processus procure des privilèges d'administrateur à un grand nombre de personnes. Il en résulte une augmentation importante des risques d'atteinte à la sécurité dus aux erreurs et à la malveillance, puisque les

administrateurs locaux peuvent activer ou réactiver les cartes temporaires d'intervenants.

De plus, des cartes d'administrateur central sont « cachées » dans les établissements en cas de problèmes pour des raisons de fonctionnement; ceci augmente les risques d'accroc à la sécurité.

7. Le nombre de personnes pouvant désactiver et réactiver les clés d'accès au système doit être limité au strict minimum.

8. Aucune carte d'administrateur central ne doit être conservée localement même pour des fins de relève. Un système centralisé doit prévoir des mesures de relève en mode dégradé et ces mesures ne doivent pas réduire le niveau global de sécurité instauré.

Un dernier aspect mérite d'être soulevé. Dans le projet de Laval, la RAMQ délègue certaines de ses responsabilités aux administrateurs locaux, employés des établissements ou des entreprises privées. Dans ce modèle, il est toutefois difficile de répartir les responsabilités de ces administrateurs et du ou des organismes responsables de l'émission des cartes d'intervenants. Qui serait imputable si un administrateur local contrevenait aux règles de conduite de l'organisme ou à une loi? Comment l'organisme s'assurera-t-il que ses « agents » adoptent la conduite prescrite?

7.2.3 Portabilité de la carte intervenant

Notre examen a révélé qu'il y a eu peu d'utilisation de cartes temporaires dans ce projet parce que beaucoup d'intervenants ont laissé leurs cartes dans les bureaux en permanence.

Cette façon de faire évite les pertes et les oublis, mais présente des lacunes en terme de sécurité. En laissant les cartes dans les bureaux, le niveau de sécurité procuré par celles-ci est ramené au niveau de sé-

curité d'un simple mécanisme d'accès logiciel et la sécurité se trouve réduite au NIP de quatre caractères.

9. La carte intervenant présente des perspectives intéressantes à des fins de contrôle d'accès, d'authentification et possiblement de scellement par le chiffrement des informations sensibles. Ce support « portable » devrait être effectivement détenu par les personnes.

7.2.4 Profil d'accès

Pour les intervenants, plusieurs profils d'accès existent. En mode lecture, ces profils concernent l'accès aux *données cléricales, données cléricales et d'urgence* et *données cléricales, d'urgence et cliniques*, alors qu'en mode mise à jour, écriture et suppression, ils concernent les *données cléricales* et les *données cléricales, d'urgence et cliniques*.

Dans le projet, l'attribution des profils était la responsabilité des établissements. Au centre médical et à la pharmacie, il fut décidé d'octroyer le même profil à tous les intervenants, soit l'accès le plus large. Une personne dans chacune des entités était responsable de transmettre les demandes à la RAMQ.

Il peut être justifié qu'une personne de confiance à l'interne authentifie les utilisateurs du système et permette l'attribution des accès. Cependant, ces accès doivent être accordés selon des règles et des critères connus et uniformes. Rappelons que les privilèges d'accès doivent être légitimes avant d'être techniquement accordés. Nous considérons que l'octroi des droits d'accès présente un risque quant à la protection des renseignements personnels. Par exemple, dans le projet, les pharmaciens avaient un accès similaire à celui des médecins. Ce privilège ne pouvait leur être octroyé sans que la démonstration de la nécessité ne soit faite en considérant notamment l'avis des ordres professionnels concernés.

10. Les privilèges d'accès doivent toujours être attribués selon des règles et des critères connus et uniformes. Ces règles et critères doivent faire en sorte qu'un intervenant de la santé ne puisse accéder qu'aux seuls renseignements personnels nécessaires à l'exercice de ses fonctions.

7.3 Appréciation du système DCS

7.3.1 Liens entre les acteurs et autonomie des établissements

Dans le cadre du projet, la RAMQ a signé des contrats[14] avec les établissements participants dans la région de Laval, avec la clinique privée et avec la pharmacie. Dans ces contrats, on exige de prendre les mesures nécessaires afin d'« *utiliser le système de Carte santé dans le respect de la vie privée des usagers et de la confidentialité des renseignements personnels auxquels ils ont ainsi accès* ». En ce qui a trait à la sécurité matérielle, logicielle et physique, la RAMQ n'impose aucune exigence aux différents acteurs du projet.

> « *L'installation des équipements est faite selon les standards établis par chaque établissement*. » - Comité de consultation, rencontre du 10 mai 2000.

Malgré le fait que les établissements du réseau de la santé, les cliniques et les pharmacies soient des entités légales distinctes, il est impératif que des mesures minimales soient mises en place. Cet aspect est important pour ne pas affaiblir la sécurité globale d'un réseau ou d'une infrastructure en branchant une entité qui constituerait le maillon faible de la chaîne. Il faut éviter par exemple que le DCS cohabite avec des systèmes de gestion personnelle à l'intervenant ou que des postes du réseau soient munis de modems. Il faut aussi s'assurer régulièrement que les mesures minimales édictées sont effectives et appliquées correctement. Pour cela, les contrats doivent contenir un droit de vérification.

L'utilisation du DCS nécessite l'installation ou l'utilisation d'équipements et de réseaux; dans les établissements, un soutien technologique et une expertise sont offerts. Les cliniques privées et les pharmacies n'ont évidemment pas accès à ce soutien. S'ils doivent acquérir ou adapter leurs équipements, réseaux et logiciels, c'est de leur propre chef et le financement est à leur charge.

[14] Chacun des contrats est intitulé « Contrat relatif au projet vitrine PRSA-carte santé ».

11. Un projet de la nature du DCS devrait exiger de ses partenaires un niveau de sécurité minimal afin de garantir le niveau global de sécurité du système. Ces exigences doivent être incluses aux ententes. De même, ces ententes doivent prévoir un droit de regard et de vérification des éléments ayant un impact sur la sécurité globale d'un tel système de la part du détenteur de l'information. Il est hasardeux de laisser le soin aux intervenants d'établir les éléments de sécurité physiques et logiques à mettre en place. Il est indispensable que les établissements de santé, les cliniques privées, les pharmacies ou autres points de service puissent bénéficier d'un soutien afin d'assurer l'implantation et le maintien de mesures de sécurité minimales.

7.3.2 Banque de données anonymes et anonymat

La RAMQ considère le DCS comme une BDA. Nous avons établi précédemment que le DCS est constitué des données sur la carte et des données concentrées à la RAMQ. Le fichier DCS inclut donc la carte qui contient les pointeurs permettant de lire le contenu d'un dossier éparpillé sur la banque de données. En logeant en des lieux différents des parties d'un dossier, celui-ci ne devient pas deux ou plusieurs dossiers distincts. L'ensemble des cartes et la BDA forment un seul et unique fichier puisque la BDA est inutilisable sans la présence de cartes. Ce fichier de renseignements personnels est nominatif et la distribution sur des supports d'entreposage n'est qu'une mesure de sécurité. L'anonymat de la BDA est ici un artifice contrôlé par la RAMQ qui pourrait modifier en tout temps ses systèmes afin de garder des traces permettant d'identifier les patients ou de dresser divers profils concernant la pratique médicale ou la consommation des soins par les patients par exemple.

Il faut aussi considérer la présence de tous les fichiers contenant des renseignements personnels constitués dans le cadre de l'administration du système et qui permettent avec plus ou moins de difficultés tech-

niques de connaître le lien entre le détenteur d'une carte et le fichier DCS : le bottin des cartes, les journaux et une éventuelle base de données de sauvegarde.
Rappelons que la RAMQ est responsable de s'assurer de la gestion du système et des différents éléments de sécurité, du succès des transactions et de la disponibilité du système. Ces obligations exigées de la RAMQ la rendent imputable de tout bris d'intégrité à l'intérieur de son système. Comment peut-elle s'assurer de la sécurité d'une banque qu'elle détient et la gérer sans prétendre y avoir accès en toutes circonstances?

De plus, il ne faut pas négliger qu'un intervenant autorisé à alimenter le DCS peut saisir du texte libre, comme il le fait dans un dossier papier à l'aide d'un stylo. Ainsi, un intervenant pourrait saisir dans un champ de la BDA des données nominatives (champ texte). Même si les intervenants rencontrés au cours de notre mandat nous affirment ne pas procéder de cette manière habituellement, il reste que l'anonymat pour l'alimentation en cours repose uniquement sur la méthode de travail et les habitudes de chaque intervenant qui inscrit des données dans le DCS.

12. La CAI souhaite que le qualificatif « anonyme » ne soit plus utilisé lorsqu'il est possible par un moyen ou un autre d'identifier une personne, lorsqu'un moyen de déduction logique permet de reconstituer une identité à partir de plusieurs renseignements anonymes, lorsque le mécanisme de dénominalisation est réversible ou lorsqu'un pseudonyme remplace un identifiant. Ce qualificatif porte à confusion et a un impact considérable sur la détermination du cadre juridique applicable à ce type de fichier.

7.3.3 Bottin des cartes et fichier des détenteurs

Lorsqu'une carte est émise, celle-ci est inscrite automatiquement dans le *bottin des cartes émises,* fichier détenu centralement par la RAMQ. Ce fichier contient les renseignements d'identité qui sont inscrits sur les cartes des patients et des intervenants. Le bottin est un fichier accessible par le réseau qui permet au système de carte santé de s'assu-

rer de la présence et de la validité de chaque carte à microprocesseur demandée et utilisée dans le système. De plus, une autre banque de données, la banque de données « personnes », est constituée et répertorie les coordonnées des détenteurs de cartes.

L'utilisation de tels fichiers soulève des questions quant à la robustesse du mécanisme d'authentification utilisé dans le projet; si on a confiance dans un mécanisme d'authentification, il est inutile de le doubler, la carte elle-même devrait suffire. Il est aisé de comprendre l'utilité d'un fichier de cartes invalides. Par contre, garder une trace de toutes les cartes émises et effectuer une validation de chaque carte à chaque utilisation annule une des caractéristiques les plus intéressantes des cartes à microprocesseur, soit la capacité à décentraliser. Ceci augmente inutilement la circulation de données avec les risques inhérents à une telle pratique.

13. La multiplication des fichiers de renseignements personnels constitués pour administrer le système DCS induit des risques supplémentaires en ce qui concerne la vie privée et la protection des renseignements personnels.

7.3.4 Consentement

Le consentement régit certes l'autorisation à communiquer, mais la première règle à suivre est celle de la nécessité. Un organisme ne pourrait donc avec un consentement recueillir des renseignements personnels sans en justifier la nécessité.

Pour être valide, un consentement à une communication de renseignements personnels se doit d'être libre, spécifique, éclairé et limité dans le temps.

Dans la présente expérimentation, le patient exprime son consentement en présentant sa carte et en saisissant son NIP.

Consentement libre : le patient est libre de présenter ou non sa carte, donc de consentir à l'accès à son DCS parce que le volet administratif est demeuré sur la traditionnelle carte d'assurance maladie. Le consen-

tement expérimenté à Laval aurait été complètement libre si les établissements et entreprises n'avaient pas eu d'indication sur le fait que la personne possède ou non une carte santé. Puisque ces organismes savaient qu'un patient était détenteur ou non d'une carte, on peut penser que l'expression du consentement n'était pas entièrement libre. Il est possible qu'un patient se sente obligé d'utiliser sa carte si le professionnel de la santé lui fait savoir que son dossier indique qu'il en est détenteur.

Consentement spécifique et éclairé : un consentement est spécifique lorsque le patient sait quels seront les intervenants qui communiqueront et recevront des renseignements le concernant. Un consentement est éclairé lorsque le patient comprend l'objet de l'échange, quels renseignements seront échangés et comment ceux-ci seront utilisés.

Le consentement obtenu lors de l'alimentation du DCS ne peut être éclairé et spécifique parce qu'un patient ne peut savoir à ce moment à quoi et où servira la communication à laquelle il consent. Le fait que l'interface de confirmation de l'information à verser au DCS n'ait pas été développée dans le cadre de l'expérimentation fait en sorte que le patient ne sait pas quelle information est versée à son DCS.

Or, bien que le consentement lors de la consultation soit spécifique, il n'est pas éclairé parce qu'avant d'autoriser l'accès au DCS, le patient ignore ce qu'il contient; il ne peut visualiser le contenu qu'une fois qu'il a donné accès.

Consentement limité dans le temps : le consentement est limité dans le temps dans la mesure où l'expérimentation procure un consentement ponctuel et qu'en retirant la carte patient du lecteur, l'accès au DCS par un intervenant devient impossible. La personne qui consent à l'alimentation du DCS ne connaît pas le contexte futur d'utilisation des données. Il est donc impossible d'établir une limite de temps au consentement même si, par la suite, un patient consent à chaque accès au DCS.

La qualité du consentement quant au contrôle du patient sur la pertinence des informations échangées ne peut être appréciée dans la présente expérimentation considérant la difficulté de cerner la finalité du DCS. Si ce dernier est contrôlé par le patient, celui-ci devrait posséder un contrôle sur l'information à communiquer d'une granularité plus

fine. S'il s'agit d'un mécanisme d'échange de renseignements cliniques entre intervenants, la pertinence devrait être déterminée par les intervenants et comme le consentement est ponctuel, la pertinence devrait aussi être déterminée de façon ponctuelle. La pertinence des informations échangées est un enjeu majeur dans le respect des règles de protection des renseignements personnels. Par exemple, pourquoi un médecin aurait-il accès à des données sur une fracture d'un membre ayant eu lieu antérieurement si un patient consulte pour une sinusite?

7.3.5 Absence de l'interface de confirmation

Le projet prévoyait que le consentement d'un patient serait confirmé par le truchement d'une interface spécifique permettant d'afficher avant l'alimentation les données qui seraient tirées du dossier local du patient pour être versées dans le DCS. Cette fonctionnalité n'a pas été implantée. Il est donc difficile pour un patient de bien comprendre et visualiser ce qui sera versé dans le DCS.

14. La CAI croit que la présence de l'interface de confirmation est fondamentale pour qu'un citoyen comprenne quelles informations circulent d'un système à l'autre.

7.3.6 Volet pharmacie – Contrôle de l'alimentation

L'interface d'alimentation du DCS développée pour la pharmacie visait à expérimenter l'exercice d'un plus grand contrôle par le citoyen sur l'information qui alimente le DCS.

Il était prévu à cet effet la possibilité suivante : « *… le pharmacien doit donc indiquer le choix du patient, en ce qui concerne l'alimentation de son DCS, pour chacun des médicaments prescrits ou pour toute la prescription complète…* »[15].

[15] Guide des fournisseurs, PROJET VITRINE PRSA – CARTE SANTÉ, Version 1.1, Direction des orientations et du développement stratégique, Régie de l'assurance maladie du Québec.

Ainsi, un patient pouvait choisir d'alimenter le DCS par médicament prescrit et non pas par ordonnance qui peut contenir plusieurs médicaments prescrits. L'interface pour ce faire était disponible mais, en pratique, ce choix n'a pas été donné au citoyen pour des questions d'ergonomie des lieux et d'impacts sur les activités commerciales; il ne pouvait qu'alimenter ou non la prescription entière. Ce volet n'a donc pu être étudié ni apprécié dans l'expérimentation de Laval.

7.3.7 Données locales et DCS

Le DCS est un dossier médical volontaire indépendant des dossiers locaux. Le système DCS est alimenté par des interfaces développées dans le cadre de la présente expérimentation servant à pomper les données des dossiers locaux et les copier dans le fichier DCS à la RAMQ. Nous avons constaté que le développement de ces interfaces implique la modification des données locales afin de repérer par la suite les données ayant alimenté le DCS ou pour les conserver en attente d'une alimentation ultérieure. Souvenons-nous que le patient peut choisir de reporter l'alimentation et mettre ses données en « réserve ». Le dossier local contient aussi une mention sur la détention ou non d'une carte santé par le patient. Nous croyons que le fait que les données locales conservent un lien avec le DCS présente des risques majeurs pour la protection des renseignements personnels. Ces liens deviennent des données locales exploitables par ces entités locales.

Ces données locales sont d'ailleurs exploitées en pharmacie où un programme exécutable nommé RapDCS.exe a été ajouté aux fins de produire un rapport intitulé « Liste des patients participant au projet vitrine PRSA – Carte santé ». Ce rapport présente les données suivantes : nom, prénom, adresse, ville, date à partir de laquelle les services sont considérés pour l'alimentation du DCS du patient. Cette pratique ne nous a pas été justifiée et cet exécutable détourne la finalité initiale des données requises pour le fonctionnement du système DCS.

L'exploitation des autres traces laissées dans les systèmes locaux pourrait aussi présenter des risques pour la vie privée en permettant par exemple la constitution de profils sur la sensibilité d'une personne à alimenter une information ou une autre.

15. La CAI considère que les dossiers cliniques locaux ne doivent contenir aucun élément susceptible de permetrre d'identifier les données ayant servi à alimenter le DCS ou celles qui pourraient l'alimenter.

7.3.8 Verrouillage des cartes

Le projet DCS prévoit que la saisie d'un NIP erroné à trois reprises verrouille la carte du patient. Cette sécurité est affaiblie par le fait qu'une carte verrouillée peut être déverrouillée par n'importe quel intervenant. Le nombre de personnes pouvant déverrouiller une carte réduit la sécurité du système.

16. Le déverrouillage des cartes patients doit être mieux encadré afin de ne pas amoindrir le niveau de sécurité.

7.3.9 Journalisation et sauvegarde

La journalisation des transactions s'est faite pour la clinique médicale et la pharmacie. Elle n'a pas été étendue aux établissements pour des raisons techniques, mais l'intention de le faire était présente. On nous a affirmé ne pas exploiter ces journaux qui sont par ailleurs incomplets. Ces nouveaux dépôts de renseignements personnels détenus par une entité centrale présentent un potentiel de risques supplémentaires de traçage, de constitution de profils et de surveillance.

Actuellement, une personne qui perd sa carte à microprocesseur doit demander l'émission d'une nouvelle carte. La carte étant la clé d'accès au fichier externe, les données contenues au DCS sont perdues de même que celles inscrites sur la carte; l'alimentation doit être reprise à zéro. Pour éviter cette situation, la RAMQ avait prévu l'instauration d'un serveur de sauvegarde dans lequel des images à jour du contenu de l'ensemble des cartes devaient être conservées, c'est-à-dire les données inscrites sur la carte, y compris les données cliniques et les pointeurs. Cette fonctionnalité n'a pas été implantée pour des raisons budgétaires. Si tel avait été le cas, la RAMQ aurait ainsi détenu la clé d'accès pour tous les utilisateurs aux données du DCS.

17. Il est important dans un tel projet d'élaborer une architecture de système qui évite la multiplication des dépôts de données contenant des renseignements personnels.

7.4 Technologie

7.4.1 Les garanties de sécurité

La technologie de carte à microprocesseur utilisée dans le système DCS s'éloigne des modèles de cartes utilisés par l'industrie. Dans le système DCS, des opérations et des traitements généralement effectués grâce au microprocesseur de la carte de façon autonome ont été déplacés vers le poste de travail. La sécurité du poste est assurée par des moyens logiciels alors que la carte est un dispositif généralement considéré comme sécuritaire parce que matériel. Ainsi, il est impossible d'attribuer les caractéristiques de sécurité normalement reconnues internationalement aux cartes à microprocesseur au système déployé par la RAMQ. Ceci nécessite que non seulement la carte, le matériel périphérique et les logiciels d'interface avec la carte soient correctement sécurisés, mais aussi que l'ensemble du système le soit. Cette sécurité ne doit pas être inférieure à ce qu'offrirait la carte à microprocesseur lorsque utilisée sans lien avec un fichier externe.

Or, pour le présent projet, la RAMQ n'a pas fait homologuer son système conformément à des normes internationales, tel qu'il est souvent d'usage dans le domaine des cartes à microprocesseur. Ce modèle, puisqu'il s'écarte des standards connus de l'industrie, se doit d'être homologué pour s'assurer qu'il offre une sécurité suffisante, ce qui ne signifierait pas par ailleurs qu'il offre des garanties suffisantes au chapitre du droit à la vie privée et à la protection des renseignements personnels.

Les informations reçues concernant le fonctionnement détaillé du système DCS sont sommaires et ne nous ont pas permis d'apprécier la sécurité cryptographique de celui-ci, cette sécurité n'étant pas basée sur la structure des échanges, mais sur la robustesse du chiffrement mis en place. Nous avons tout de même identifié des éléments du système qui pourraient présenter des risques et qui doivent être évalués dans le cadre d'une homologation ou d'une certification officielle et indépendante :

- la clé système inscrite dans les registres de chaque machine multiplie les possibilités de s'emparer de cette clé et de la décoder;

- l'absence de chiffrement entre le poste et la carte introduit une vulnérabilité d'interception;

- la sécurité se trouve basée sur le logiciel VigiMaître qui déplace les traitements sur le poste plutôt que sur la carte en ramenant la sécurité globale à celle du poste de travail. Cette sécurité logicielle est nécessairement moindre que si les traitements étaient effectués sur la carte;

- l'introduction de fichiers externes et l'importance stratégique, ce faisant, de la synchronisation des pointeurs, un pointeur désynchronisé pointerait alors au mauvais endroit dans le fichier entreposé à la RAMQ. Imaginons un instant l'impact d'une désynchronisation de pointeurs qui résulte en un mélange de différents dossiers de patients, en la possibilité de divulgation de renseignements cliniques certes, mais surtout en des risques pour la santé du patient dont le dossier est désynchronisé;

- l'importance de la robustesse du générateur de valeur aléatoire doit être évaluée afin d'assurer la fiabilité d'utilisation d'un algorithme de chiffrement normalisé.

En France, le gouvernement a déployé un système de cartes à microprocesseur qui sert à des fins administratives (remboursement des assurés) dans le secteur de la santé. Ce système utilise, un peu comme le système DCS, des cartes à microprocesseur (sans indexage) pour les patients (carte Vitale) et des cartes pour les intervenants (carte CPS ou carte de professionnel de santé). Or, une rigoureuse procédure d'homologation de tous les produits matériels et logiciels utilisés et utilisables par ce système a été mise en place. Cette homologation nécessite des tests de produits par des laboratoires indépendants référencés par le Groupe d'intérêt économique (GIE) SESAM-Vitale, qui s'occupe principalement de la carte utilisateur et le GIE CPS[16] qui s'occupe des

[16] La famille CPS comprend plusieurs types de cartes : carte de professionnel en formation (CPF), carte de directeur d'établissement (CDE) et carte de personnel d'établissement (CPE), carte de personnel autorisé (CPA), carte de serveur applicatif (CSA), carte de

cartes des intervenants de la santé. Dépendant du produit étudié, l'homologation peut comprendre des tests électriques et différents tests fonctionnels y incluant des tests d'étanchéité. De plus, le Centre national de dépôt et d'agrément (CNDA) est chargé de réaliser des tests techniques et fonctionnels des modules de service SESAM-Vitale et du logiciel lecteur de cartes.

18. Si la RAMQ décidait de développer un système qui utilise la même technologie que celle utilisée lors du projet de Laval, elle doit faire certifier ou homologuer son système par un organisme neutre et indépendant et à un niveau suffisamment élevé pour ce type d'application[17] et ceci pour garantir la sécurité du système. Cette condition est d'autant plus importante compte tenu de l'implication de la RAMQ à titre d'actionnaire dans le développement de cette technologie.

17

7.4.2 Expertise et contrôle effectif du niveau de protection

Le projet DCS a été réalisé en collaboration avec la firme Motus. Le présent examen a permis de constater que l'expertise des produits utilisés dans l'expérimentation de Laval réside presque entièrement chez Motus. La dépendance et la captivité d'un organisme gouvernemental induit une perte de contrôle sur le traitement et la protection des renseignements personnels qui n'est pas sans inquiéter la CAI.

19. Nous croyons que la RAMQ, afin d'exercer le contrôle effectif sur la protection des renseignements personnels circulant dans le cadre du système DCS ou de tout autre système utilisant des cartes à microprocesseur, se doit de développer une expertise interne en matière de cartes à microprocesseur et de systèmes associés.

professionnel de santé (CPS). Pour cette dernière (CPS), il existe une carte par profession (médecin, pharmacien, infirmier, infirmière, chirurgien-dentiste, pédicure-podologue, psychomotricien, sage-femme, masseur kinésithérapeute, opticien, orthophoniste et ergothérapeute).

[17] Par exemple, la certification selon les critères communs (CC) permet d'attribuer un niveau d'assurance croissant à un produit qui s'étend de EAL1 à EAL7. Au Canada, le Centre de la sécurité des télécommunications offre un service d'évaluation et de certification basé sur les critères communs.

8. CONCLUSION

De façon générale, l'évaluation du projet ne permet pas à la CAI de conclure que l'expérimentation a été réalisée dans le respect de la protection des renseignements personnels.

Le présent examen de l'expérimentation de carte santé à microprocesseur de Laval réalisée par la RAMQ soulève plusieurs questions. Ces dernières seraient identiques même si le nombre de cartes utilisées dans le projet avait été plus élevé.

La première consiste à circonscrire le DCS sur le plan conceptuel et juridique : l'encadrement juridique applicable, la détermination des finalités d'un tel système, l'opportunité pour la RAMQ, dans ses missions multiples, de détenir un fichier de renseignements cliniques et la détermination des risques pour les citoyens de confier, à la RAMQ, la gestion d'une nouvelle mégabanque de données contenant des données particulièrement sensibles au sujet des citoyens.

La seconde vise à circonscrire, sur le plan conceptuel et juridique, le système d'habilitation expérimenté à Laval : l'encadrement juridique applicable et l'opportunité pour la RAMQ de constituer un fichier de renseignements personnels sur les intervenants en santé, qu'ils soient dispensateurs de soins ou non.

La troisième se rapporte à la détermination du caractère dit anonyme de la banque de données créée et détenue par la RAMQ. Présentement, de nombreuses interprétations du terme « anonyme » circulent. Or, l'intérêt de cette définition n'a rien de sémantique. S'il est toujours possible d'identifier une personne, que cette identification soit faite par la RAMQ ou qui que ce soit d'autre, on ne doit pas parler du caractère anonyme d'une banque de données. L'utilisation du terme anonyme laisse croire au citoyen que ses renseignements de nature médicale sont à l'abri de toute divulgation, alors que tel n'est pas le cas.

La quatrième consiste à obtenir une homologation indépendante et reconnue de la sécurité d'un système à carte à microprocesseur en

marge de l'industrie. Cette recommandation est d'autant plus justifiée si l'on considère l'intérêt de la RAMQ dans le développement des produits en cause. En parallèle, rappelons l'importance de développer à l'interne une expertise technologique évitant ainsi la captivité et la dépendance d'une firme externe.

Cette liste d'éléments démontre que de nombreux fils restent à attacher et qu'on ne peut considérer la présente expérience comme concluante et garante de la protection des renseignements personnels.

Devant une telle situation, la CAI ne peut que réitérer son souhait de la tenue d'un véritable débat public, tel que s'y était d'ailleurs engagé le gouvernement sur recommandation du ministre de la Santé et des Services sociaux dans le décret 1177-99 du 13 octobre 1999. Ce débat devrait largement déborder l'opportunité de réaliser un projet d'utilisation d'une carte à microprocesseur et porter sur les changements qui ont cours dans le modèle de prestation des soins de santé et sur les impacts que ces façons de faire ont sur le droit à la vie privée des citoyens et sur l'exercice du secret professionnel par les professionnels de la santé.