Les enjeux et risques juridiques des échanges d'information dans la relation patient-médecin dans l'espace santé TELUS

Pierre TRUDEL

France ABRAN

Étude menée dans le cadre du programme « *Ma première ligne numérique en santé* » du CEFRIO

1er février 2016

CENTRE DE RECHERCHE EN DROIT PUBLIC

Faculté de droit
Université de Montréal

Table des matières

Introduction

L'espace santé TELUS est une plate-forme infonuagique, certifiée et sécurisée, permettant de recueillir, stocker, utiliser et partager des renseignements de santé en ligne. Cette plate-forme, optimisée par *Microsoft HealthVault*, permet aux individus d'emmagasiner toute information de santé ou de mieux-être et d'en permettre le partage avec des applications ou d'autres utilisateurs autorisés.

Un vaste ensemble d'information peuvent être stockées dans l'espace santé TELUS : dossier d'hospitalisation ou de consultation médicale, médicaments, dossier de vaccination, résultats d'analyses en laboratoire, données provenant d'appareils médicaux (ex : podomètre, glycomètre, tensiomètre artériel…) ou d'applications logicielles branchées à l'espace santé TELUS (ex : outil de gestion des maladies chroniques, application d'entraînement physique, de perte de poids ou de pression artérielle…)

L'espace santé TELUS est la technologie qui permet le fonctionnement de cette «plate-forme partagée de données en ligne» à laquelle on peut accéder par de multiples applications et appareils afin de prendre connaissance des renseignements de santé d'une personne. L'espace santé personnel (ESP), comme le projet de la clinique Nouvelle Beauce, est une application branchée à l'espace santé TELUS qui permet de rassembler, de stocker et d'organiser les renseignements de santé du patient dans un dossier unique centralisé. Le patient ou son représentant autorisé peut consulter, utiliser et aussi partager, en tout ou en partie, les données de son dossier de santé avec des tiers (parents, amis ou autres) ou des fournisseurs de soins de santé.

Le présent rapport présente une analyse des enjeux et risques associés à l'application espace santé TELUS telle que présentée dans le cadre du projet. L'analyse résulte de l'examen de la configuration générale et du fonctionnement de l'espace santé TELUS au regard des exigences des lois applicables au Québec.

Dans le premier chapitre, il est fait état des caractéristiques des environnements connectés que constituent les environnements de e-santé de même que les mutations qu'elles supposent dans le champ de la relation entre les patients et les personnels soignants. On y explique aussi les exigences inhérentes à l'évaluation de leurs enjeux et risques juridiques de même que le cadre d'analyse qui est appliqué.

Au chapitre deuxième, l'on explique les principales caractéristiques de l'espace santé TELUS tel qu'il a été utilisé dans le cadre du projet de recherche. On passe en revue les principales composantes de cet environnement technologique, le contexte dans lequel il se déploie de même que les principales fonctions et activités qu'il peut supporter. Cela permet d'identifier les enjeux généraux de l'espace santé personnel au regard notamment des données médicales qui y sont consignées ainsi qu'aux possibilités de partage de ces données.

Au troisième chapitre, les enjeux et risques sont signalés en présentant les différentes phases du cycle de fonctionnement de l'espace santé TELUS. On fait état des principales situations qui surviennent tout au long du cycle d'utilisation de l'espace santé par un participant. Cela permet de décrire les dispositions applicables de la législation québécoise lors des différentes situations relatives à un document se trouvant dans un tel environnement ou qui est utilisé dans le cadre d'échanges et de transactions. On passe ainsi en revue le processus d'ouverture du compte par les participants et les enjeux relatifs à l'identification des participants. On envisage le déroulement des différentes étapes qui se caractérisent par le dépôt et le traitement de documents de même que leur partage. Les enjeux relatifs à la transmission d'un document de l'espace santé personnel, la signature de celui-ci

de même que les enjeux relatifs à la fin de l'utilisation de l'espace santé par le participant sont aussi examinés.

Le quatrième chapitre est consacré à l'analyse des responsabilités des acteurs impliqués dans l'espace santé, à savoir les participants, la clinique et les professionnels de la santé et bien évidemment le prestataire de service qui constitue un acteur inédit dans le schéma classique de la relation de soins.

Pour effectuer les analyses présentées dans ce rapport, il a été postulé que les fonctions annoncées de l'espace santé (encryptage, horodatage etc.) fonctionnent normalement et sont utilisées en conformité avec les spécifications techniques qui leur sont applicables. Ces fonctions ont été examinées au regard des exigences et prescriptions des lois applicables au Québec.

De cette démarche ont été identifiés des enjeux et des risques qui doivent être considérés par les différents participants au projet pilote. Ce sont ces enjeux et risques qui sont traités ci-après avec les précautions envisageables afin d'y répondre.

1. Le cadre d'analyse des enjeux et risques juridiques des environnements de e-santé

La plate-forme TELUS avec les possibilités qu'elle procure de disposer d'un d'espace santé personnel (ESP) est emblématique des mutations du schéma classique de la production et de la circulation de l'information dans le contexte des relations associées aux soins de santé.

Il s'agit d'un environnement en grande partie sous la maîtrise du patient ou des proches de celui-ci. C'est un outil informationnel de e-santé destiné à l'aider à mieux gérer les informations relatives à la santé des individus.

Les possibilités que confère cette plate-forme en habilitant le patient à autoriser le versement d'information sur son état de santé et les différentes possibilités de partager et d'ajouter à ces informations contribuent à la rattacher à la catégorie émergente des systèmes de données de santé générées par les patients [Patient-Generated Health Data (PGHD)][1].

Les systèmes de données de santé générées par les patients contribuent à redéfinir plusieurs des conditions de la relation entre le patient, les professionnels de la santé de même que les organisations impliquées dans les soins de santé. Les auteurs Shapiro, Johnston, Wald et Mon expliquent que :

> *Patient-generated health data (PGHD) are health-related data—including health history, symptoms, biometric data, treatment history, lifestyle choices, and other information—created, recorded, gathered, or inferred by or from patients or their designees (i.e., care partners or those who assist them) to help address a health concern. PGHD are distinct from data generated in clinical settings and through encounters with providers in two important ways. First, patients, not providers, are primarily responsible for capturing or recording these data. Second, patients direct the sharing or distributing of these data to health care providers and other stakeholders.*[2]

Un grand nombre d'applications de e-santé sont a priori destinées aux personnes désireuses de connaître et analyser des informations relatives à leur propre condition physique. Par exemple, des capteurs de données installés sur les corps produisent des informations sur le comportement de celui-ci, les symptômes, les taux de telles ou telles substances corporelles.

On relève aussi l'avènement d'une autre catégorie d'applications orientées celles-là vers le suivi en temps réel du patient ou l'administration de traitements à distance.

Les outils connectés en réseaux et des dispositifs portables connectés facilitent la collecte, la conservation, la compilation et la communication de données relatives à la santé des patients. Par exemple, à l'aide d'applications ou de dispositifs connectés, le patient peut recueillir ses données de santé (poids, pression artérielle, glycémie, pourcentage de graisse…) sur plusieurs mois et ces données pourront être récupérées par son médecin, et ce pour faciliter la prévention ou le diagnostic. L'espace santé permet de telles interconnections avec des dispositifs implantés ou portés qui peuvent capter, transmettre ou générer des informations. Mais dans les expériences réalisées dans le cadre du présent projet, ces fonctions n'ont pas été analysées.

---

1 Voir notamment : Fréderic Durand Salmon et Loïc LeTallec, « La e-santé : de nouveaux usages pour les technologies individuelles en santé publique », *Réalités industrielles (Annales de l'École des Mines)*, Novembre 2014, 70-75.

2 Shapiro, M., D. Johnston, J. Wald et D. Mon, *Patient-Generated Health Data- White Paper*, prepared for Office of Policy and Planning Office of the National Coordinator for Health Information Technology, RTI International, April 2013, p. 2.

Les environnements qui émergent désormais sont caractérisés par leur inclusion dans des **environnements en réseau**.

On entend par environnement en réseau, un ensemble de personnes et de lieux décisionnels reliés entre eux par des moyens informatiques. La communication électronique est possible grâce à la mise en place de raccordements entre les différents terminaux de tous ceux qui veulent entrer en communication : c'est la notion de réseau[3]. La constitution de réseaux permet de raccorder les correspondants; ces réseaux peuvent être eux-mêmes raccordés à d'autres réseaux et donner un accès à une multitude de correspondants. Le réseau est l'élément névralgique de cet environnement virtuel appelé «cyberespace».

Le mot «réseau» a un sens très étendu. Il est ainsi défini dans le dictionnaire Robert :

> *Ensemble des lignes, des voies de communication, des conducteurs électriques, des canalisations, etc. qui desservent une même unité géographique.* [...] *Répartition des éléments d'une organisation en différents points; ces éléments ainsi répartis*[4].

Deux sens à la notion de réseau sont susceptibles d'avoir un écho lorsqu'il est question d'un espace de communication entre patients et professionnels de la santé. Le mot a une signification qui nous renvoie dans le champ technique lorsqu'on réfère aux ensembles de conduits de lignes de télécommunication. Alors un réseau serait l'ensemble résultant d'une ou plusieurs interconnexions et possédant une capacité de transmettre ou de diffuser le même contenu. Un autre sens réfère plutôt au concept d'organisation. Le réseau serait alors cet ensemble d'éléments réunis par différents liens de nature organisationnelle. Il pourrait s'agir de liens physiques ou simplement organisationnels.

Si les *possibilités physiques* sont nécessaires à l'existence d'un réseau, elles ne sont pas suffisantes. Un réseau existe moyennant la volonté des parties d'y adhérer. Les volontés de s'y raccorder sont évidemment rendues possibles par l'existence de protocoles techniques mais elles se manifestent généralement en raison de finalités poursuivies par les acteurs. Autrement dit, on se raccorde à un réseau afin de bénéficier des avantages résultant d'un tel raccordement. Il y a donc, chez ceux qui participent à l'environnement réseau, un certain «vouloir communiquer collectif», une sorte de *volonté d'interaction* qui est l'autre composante de l'environnement réseau.

Afin de bien cerner les dynamiques qui se manifestent dans le cyberespace, il est donc utile d'envisager les réseaux comme des *ensembles d'usagers interconnectés*. La notion inclut évidemment les fournisseurs d'accès à l'environnement en réseau et les autres fournisseurs de capacités de transmissions et de connectivité. Elle recouvre également une autre notion, celle des groupes ou sous-groupes qui se créent dans l'environnement réseau. Ils forment en quelque sorte une communauté d'intérêt, à tout le moins pour les questions qui sont l'objet d'un lieu d'interaction précis, en l'occurrence ici l'état de santé des personnes concernées.

Ainsi, un environnement comme l'ESP constitue un réseau en ce qu'il a pour finalité de mettre en relation, parfois en présence, un ensemble d'acteurs dotés de capacités de prendre des décisions ayant un effet sur les autres.

---

[3] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 2-3.

[4] LE PETIT ROBERT 1, *Dictionnaire alphabétique et analogique de la langue française*, Paris, Dictionnaire Le Robert, 1990.

La possibilité de doter les moindres objets d'une capacité de raccordement au réseau emporte la nécessité de penser leur cadre juridique en les envisageant comme autant d'objets pouvant capter, conserver et communiquer de l'information et raccordés en réseau, donc capables d'interactions.

Rendre compte du cadre juridique des environnements de santé connectés suppose de déterminer dans quelle mesure s'appliquent les lois qui encadrent la collecte, la circulation et les autres traitements d'information. Mais il faut aller plus loin : il est nécessaire d'analyser le cadre juridique en s'interrogeant sur les enjeux et les risques qu'induit la connectivité au réseau, compte tenu des caractéristiques propres aux informations de santé.

Pour envisager l'encadrement normatif des environnements de e-santé dans le contexte des risques que la technologie paraît induire, il faut partir des caractéristiques et des logiques de fonctionnement de ces environnements. Cela permet d'identifier les enjeux que posent ces environnements connectés et de se donner les moyens d'identifier les encadrements juridiques qui sont concernés.

Lorsque l'on met en place des réseaux, il importe d'organiser l'espace au sein duquel les données peuvent circuler. Le cadre juridique régissant la gestion des informations définit les droits et les responsabilités des patients, des professionnels et des prestataires impliqués dans l'hébergement des données et les diverses opérations relatives à l'accès par les personnes habilitées. Les protections sont conçues de manière à garantir que les données seront effectivement utilisées pour des fins identifiées, plutôt que pour empêcher platement leur circulation. Au plan juridique, l'on obtient un espace régulé. Au plan technique, c'est un espace normé. Ce régime juridique permet de situer les protections qui doivent être assurées à l'égard des données personnelles là où se situent les vrais enjeux. Le cadre juridique permet aussi de préciser les responsabilités respectives de tous ceux qui se trouvent à en avoir la maîtrise au sein d'un espace en réseau[5].

À l'égard de la vie privée, du secret médical et des autres droits des personnes concernées, la régulation de ces environnements connectés se présente comme un ensemble de décisions de gestion des risques qui sont perçus par les acteurs au sein des réseaux.

Lorsqu'on entreprend d'identifier de façon proactive les défis associés à ces modes de traitement de l'information de santé au regard des droits et obligations des professionnels de la santé, des patients et des autres acteurs, il importe de repérer et de caractériser les enjeux et les risques que posent l'avènement et la généralisation de tels environnements.

Au nombre des enjeux à identifier il y a notamment ceux qui sont relatifs:

- aux droits et responsabilités des acteurs impliqués dans la production, la collecte, le traitement, la transmission et la conservation de l'information;

- aux conséquences, au plan des droits et obligations, du fait que le patient est en possession et souvent en position de contrôle des interfaces utilisées dans le traitement de l'information;

- à la répartition des risques et responsabilités entre les différents acteurs de ce qui constitue pratiquement un réseau de partage de données de santé.

---

5 Pierre TRUDEL, « Aperçu du cadre juridique des services d'hébergement des données de santé », dans *Après le projet de loi 83 : un nouveau réseau de la santé*, 2006, Service de la formation continue, Barreau du Québec, 2006, EYB2006DEV1256.

- aux conditions de validation de l'information et les garanties d'intégrité et d'authenticité qui sont nécessaires, compte tenu du degré de sensibilité des différentes informations de santé.

Et ces enjeux juridiques doivent aussi être analysés en tenant compte du caractère supra-légal de plusieurs droits fondamentaux des personnes qui sont concernés par la production et la circulation de l'information dans les réseaux de e-santé.

Dans le contexte des réseaux, contrairement à ce que postulent les cadres juridiques actuels, la protection effective des données suppose d'en encadrer la dissémination et agir sur l'accès aux renseignements où qu'ils se trouvent au sein des réseaux. Il faut mettre en place un cadre juridique évitant la duplication des renseignements personnels. Ainsi, dans le contexte où les services de santé fonctionnent en réseau, le cadre juridique doit autoriser l'accès conditionnel et balisé aux données détenues en quelque point du réseau plutôt que de contraindre à la recollecte des mêmes informations.

Ces mutations portent à rechercher un modèle de réglementation qui visera à baliser le partage d'information[6]. Il s'agit d'organiser l'espace au sein duquel les données personnelles peuvent circuler. Le cadre qui en découle définit les droits et les responsabilités. Les protections sont conçues de manière à garantir que les données personnelles seront effectivement utilisées pour des fins licites, plutôt que pour empêcher leur circulation. Et le cadre situe les responsabilités respectives de tous ceux qui se trouvent à en avoir la maîtrise au sein d'un espace en réseau.

Le régime juridique doit nécessairement respecter les principes fondamentaux en matière de protection des données personnelles et de secret médical. Ces principes sont énoncés non seulement dans la législation mais résultent de documents internationaux auxquels il importe de se conformer. Il doit garantir une protection de bout en bout et assurer que seules les informations autorisées seront utilisées lors de chacune des prestations de service.

Les responsables et les responsabilités qui leur incombent doivent être identifiés. Il faut, en tout temps, être en mesure de connaître qui répond des informations personnelles détenues dans le réseau et quels sont ses devoirs. En outre, lors de chaque interaction, les participants sont informés ou ont accès aux informations à l'égard de ce qu'il advient de leurs renseignements personnels.

En tant qu'espace régulé, le réseau est nécessairement balisé par les finalités de la famille de services et prestations pour lesquelles elle est établie. Le participant est informé de sa vocation, de sa portée et de sa teneur.

L'ESP constitue donc un environnement réseau de collecte, de partage et de gestion d'information relative à la santé des personnes qui y participent. À ce titre, il est porteur d'enjeux; son utilisation de même que les capacités qu'il procure génèrent des risques pour les personnes et les organisations qui y réalisent des activités ou participent aux échanges qu'il rend possibles.

1.1 L'appréhension des enjeux de la e-santé : la gestion des risques

Pour appréhender les enjeux et risques des environnements de production et d'échange d'informations, dont les ESP, il est nécessaire de se situer dans une perspective qui va plus loin que la simple description de ce que permettent ou interdisent les lois en vigueur. Il n'est pas non plus utile de s'en remettre seulement à une recension de décisions judiciaires qui seraient susceptibles de

[6] Pierre TRUDEL, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles, » [2004] 110 *Revue française d'administration publique*, pp. 257-266.

concerner l'un ou l'autre des volets d'un système technologique comme ceux qui sont utilisés dans la e-santé.

Comme le recommandent certains auteurs, il importe de passer d'une démarche fondée sur la « résolution de problèmes » à une approche de « gestion des risques juridiques ».

Dans un environnement caractérisé par les relations en réseaux, la nature même de l'application du droit paraît connaître des changements. Alors que l'on postulait que l'application du droit consiste à appliquer la règle appropriée afin de résoudre un problème, on tend de plus en plus vers une démarche d'identification et de gestion des « risques » qui peuvent découler directement ou indirectement des règles de droit.

Richard Susskind explique que le principal aspect du travail des juristes, le *« legal problem solving* », va perdre de son importance. L'emphase va être mis davantage sur le «*legal risk management*». Une telle tendance accentue l'importance des méthodes afin de gérer les risques juridiques. Susskind explique que :

> *"In conventional, reactive legal service, when a legal risk has been perceived and a lawyer instructed, there is an expectation that some optimum disposal of the matter will be achieved. In contrast, legal risk management techniques are often brought to bear in respect of legal risks that would otherwise not be managed at all or would be addressed too late. And in this context, in the latent legal market, it may be entirely tolerable (commercially and as a matter of practicality) that any solution reached may be well short of the optimum position. The point is that the legal risk is being managed. Without such techniques, such risks would not have been managed at all or may not have been manageable. Thus there can be improvement if not perfection"*[7].

Le phénomène paraît particulièrement présent dans les environnements qui ne semblent pas posséder de limites spatio-temporelles facilement identifiables comme les réseaux interconnectés dans lesquels se déroulent des activités.

Dans ces contextes, les moindres activités sont théoriquement visées par une multitude de règles de droit de même que par d'autres normativités. Alors, la démarche encyclopédique consistant à identifier toutes et chacune des règles (théoriquement, les lois de tous les pays) et à déterminer laquelle ou lesquelles trouve application peut être supplantée par une analyse des risques que s'appliquent certaines règles ou les risques que ces dernières emportent des conséquences adverses.

Le risque juridique vient rendre compte de la relative incertitude qui peut exister quant aux conditions d'application d'une norme et quant au sens de celle-ci[8]. C'est pourquoi l'on retient que le risque juridique est engendré par l'incertitude. L'incertitude quant au cadre juridique et à son application apparaît souvent comme l'un des risques majeurs à considérer lors du déploiement de services dans des environnements inédits comme les réseaux informatiques.

Par exemple, à l'égard de l'analyse des enjeux et risques d'un système de PGHD ou d'ESP, cette analyse doit évidemment tenir compte des obligations imposées par la loi. C'est dans la Loi que l'on trouve les obligations fondamentales à partir desquelles se situe nécessairement une analyse de risques. Mais une telle démarche suppose d'identifier non seulement les exigences des lois qui s'appliquent spécifiquement aux situation visées mais également les obligations plus floues résultant

---

7 Richard SUSSKIND, *The Future of Law: Facing the Challenges of Information Technology*, Oxford University Press, 1998, p. 27.

8 Pierre TRUDEL, « Le risque, fondement et facteur d'effectivité du droit », dans Karim BENYEKHLEF, *Gouvernance et risque - Les défis de la régulation dans un monde global*, Montréal, Thémis, 241-271.

des devoirs de prudence et de diligence qui sont considérés lorsqu'est mise en cause la responsabilité d'un professionnel de la santé.

L'analyse de risques des environnements d'information consiste habituellement à identifier, à partir des gisements, des flux et de l'utilisation envisagée des informations, ce qui présente des risques pour la protection de la vie privée. Elle vise aussi à déterminer l'étendue des précautions à prendre aux fins de maîtriser les risques.

Une telle démarche permet de tenir compte des situations présentant des risques devant être pris en charge et de fournir, le cas échéant, une indication des niveaux de risques à considérer[9]. Bien qu'il soit généralement impossible de quantifier de façon chiffrée, les risques d'atteintes à la vie privée, il est possible d'indiquer que telle ou telle situation comporte un risque faible, moyen ou élevé et d'identifier les mesures prises ou à envisager pour y faire face.

1.1.1 Le risque

Dans la postmodernité, le risque apparaît comme une composante majeure de la reconfiguration des processus délibératifs associés à la production du droit. La notion de risque a d'ailleurs pris beaucoup de place dans la recherche en sciences humaines au cours de la dernière décennie[10]. Les perceptions diverses ou convergentes au sujet des risques, leur existence ou leur ampleur contribuent à construire les légitimations sur lesquelles se fondent les règles de droit. L'anticipation, la gestion et la répartition des risques figurent parmi les grandes préoccupations des systèmes juridiques. Ulrich Beck expliquait que :

> *Modern society has become a risk society […] because the fact of discussing the risks that society produces itself, anticipating them and managing them has gradually become one of society's leading concerns.*[11]

Dans une telle logique, il en découle que le droit en général et la régulation des ESP en particulier peuvent être envisagés à la lumière des risques qui tendent à le justifier ou à le légitimer. Pierret explique à cet égard que le risque apparaît comme central dans les processus de décision vis-à-vis d'un futur largement ouvert débarrassé des croyances, des traditions et du destin. « Il représente cette période intermédiaire entre la sécurité et la destruction où la perception de menaces détermine notre pensée et notre action »[12]. Ce qui amène Ewald et Kessler à relever que « l'exigence que les politiques modernes se réfléchissent comme allocation optimale des risques. »[13]

---

9 Pierre TRUDEL et France ABRAN, *Guide pour un usage responsable d'Internet à l'intention des responsables des lieux d'accès publics à Internet et des utilisateurs,* réalisé pour le Ministère de l'éducation et la Direction de l'Autoroute de l'Information du Conseil du trésor, Montréal, avril 2003, en ligne à < http://www.droitsurinternet.ca/versions.html >.

10 Jonathan JACKSON, Nick ALLUM and George GASKELL*, Perceptions of Risk in Cyberspace*, Cyber Trust & Crime Prevention Project, 04-06-2004, < http://www.foresight.gov.uk/OurWork/CompletedProjects/CyberTrust/Docs/Perceptions_of_Risk_in_Cyberspace.asp >, visité le 8 juillet 2010.

11 Ulrich BECK, "Risque et société," in Sylvie MESURE and Patrick SAVIDAN, *Le dictionnaire des sciences humaines*, (Paris: Quadrige, PUF, dicos poche, 2006), p. 1022. [Our translation.]

12 Julien PIERET, *D'une société du risque vers un droit réflexif? Illustration à partir d'un avant projet de loi relatif à l'aéroport de Zaventem*, séminaire Suis-je l'État? Séminaire virtuel de l'ULB, < http://dev.ulb.ac.be/droitpublic/index.php?id=14&tx_ttnews%5Bpointer%5D=2&cHash=d0d8282540 >, p. 5.

13 François EWALD et Denis KESSLER, « Les noces du risque et de la politique », *Le Débat*, no. 109, p. 55., cité par Pieret, p. 5.

Ainsi, penser le droit et la régulation des environnements de PGHD et d'ESP dans le contexte postmoderne nécessite de penser en termes de gestion des risques.

Le risque en tant que construction sociale sera apprécié de façon différente selon les époques et selon le contexte culturel, politique ou social[14]. Les représentations des dangers et des bienfaits des technologies contribuent à la construction des perceptions collectives des risques et des bénéfices des objets techniques. Ces perceptions varient dans le temps : elles ne sont pas identiques à toutes les époques. Elles diffèrent également selon les contextes sociaux : le droit et les autres normativités procèdent en grande partie de ces perceptions variables reflétant les contextes sociétaux et historiques.

Les acteurs évaluent les risques qu'une mesure ou une règle s'applique à leur activité. La décision de se conformer à telle règle et pas à d'autres procède d'une démarche d'évaluation des risques juridiques. Le potentiel d'application du droit de tel ordre juridique est évalué par chacun des acteurs en fonction de divers facteurs tels que les possibilités effectives de poursuites, la possession d'actifs sur le territoire étatique concerné, le désir d'inspirer confiance ou de se comporter en « bon citoyen ». Ces facteurs concourent aux analyses par lesquelles les acteurs orientent leurs stratégies de gestion de risques.

Tobias Mahler définit ainsi le risque juridique envisagé au niveau des sujets de droit: « A risk is a legal risk if its source involves a legal norm. Thus the risk needs to be the manifestation of a legal norm's potential detriment. Both factual and legal uncertainty may influence legal risk »[15]. Mahler définit la gestion du risque juridique comme étant une méthodologie consistant en un ensemble d'activités de gestion de certains types de risques, à savoir les risques découlant de la loi et les risques qui peuvent être traités (gérés) par des moyens juridiques.

La gestion du risque juridique est ainsi comprise comme visant deux types de risques que les professionnels du droit peuvent aider à identifier et à baliser à savoir les risques découlant de la loi et ceux qui peuvent être balisés en faisant appel à des solutions juridiques[16].

Le risque juridique découle en effet des situations où la violation des droits d'autrui est susceptible de se produire. Même s'ils sont différents, il y a une étroite proximité entre le risque technologique et le risque juridique : lorsque le risque technologique est avéré, il naît presque toujours une obligation d'en tenir compte et de se comporter de façon conséquente. Le risque juridique peut aussi découler de la possible non-conformité à une loi ou à une autre sorte d'obligation également applicable comme un contrat.

Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause. C'est dire l'importance d'évaluer les enjeux et risques juridiques lors de la conception, de la planification et de la mise en place de projets d'ESP.

---

14 Christine NOIVILLE, *Du bon gouvernement des risques*, Paris PUF, les voies du droit, 235 p.

15 Tobias MAHLER, « Defining Legal Risk », in Proceedings of the Conference 'Commercial Contracting for Strategic Advantage- Potentials and Prospects', Turku, University of Applied Sciences, 2007, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014364 >.

16 C. COLLARD, "*Le risque juridique existe-t-il ? Contribution à la définition du risque juridique* ", JCP, Cah. dr. ent. 2008, n° 1 (numéro spécial sur le risque juridique), pp. 8-13.

1.1.2 La modification de l'échelle des risques

Les environnements de e-santé induisent des changements dans l'échelle des risques associés aussi bien aux environnements d'information qu'à ceux qui sont inhérents à la relation entre le patient et les personnes soignantes.

Dans les environnements de e-santé, les repères spatiaux et temporels sont modifiés. Les balises conçues dans un monde dans lequel les réseaux prenaient moins de place sont prises en défaut. Des enjeux inédits dans le monde physique se manifestent avec une grande acuité dans l'espace en réseaux[17].

Certes, les relations entre les patients et les professionnels qui dispensent des soins prennent forcément place dans des lieux privés. Mais les repères permettant de délimiter les espaces privatifs des autres peuvent aisément se retrouver brouillés.

Belgum rappelle que :

> *Personal data, such as address, phone number, income, poperty value, and marital status have always been avalable to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all internet users – to gain access to similar types of personal information at little or no cost.*[18]

En particulier, les *espaces de la clinique se trouvent redéfinis* : le fait que l'information circule en flux continu entre les terminaux en possession du patient et ceux de la clinique peut induire des mutations quant aux conditions du déroulement de la relation de soins.

L'échelle spatiale à partir de laquelle s'apprécient les risques pour la vie privée et les autres droits des patients se trouve également modifiée. Beaucoup d'informations sont à portée d'une requête de moteur de recherche.

Il y a aussi un décentrage temporel : la *persistance de l'information* emporte que celle-ci traverse les cercles dans lesquelles elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible à un membre de l'équipe soignante en raison d'un événement spécifique. L'archivage et la disponibilité virtuellement permanente irait au-delà de ce qui est nécessaire afin d'assurer un suivi pertinent et cohérent.

Les capacités d'agglomération d'information permettent la constitution de gisements d'informations sur les personnes qui peuvent du coup devenir disponibles pour des forces de police de même que pour d'autres acteurs, comme les assureurs.

En somme la disponibilité en flot continu d'information sur la condition d'une personne limite évidemment les efforts à consacrer pour trouver l'information. Mais cela emporte la disparition d'une certaine protection par défaut pour la vie privée.

Tous ces changements indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau. Ces dimensionnements nouveaux induisent des mutations au niveau de la raison d'être des règles de droit et des précautions encadrant les processus de gestion de l'information.

---

17 Frederick SCHAUER, « Internet Privacy and the Public-Private Distinction », [1998] 38 *Jurimetrics* 555 ;

18 Karl D. BELGUM, « Who leads at Half-time ?: Three Conflicting Visions of Internet Privacy Policy [1999] 6 *Rich. J.L. & Tech*. 1.

Là où l'on prenait pour acquis que le niveau de risques pour la vie privée demeurait faible ou aisément maîtrisé, les mutations dans l'échelle qualitative et temporelle qu'induit la e-santé, conduit à postuler que les risques sont accrus.

D'où l'intérêt d'un renforcement de la protection de la vie privée des personnes lors de la mise en place de tels environnements de traitement de l'information.

La virtualisation de la relation patient-médecin et autres soignants emporte aussi des conséquences quant aux conditions dans lesquelles se déroule le relation de soins elle-même. Au modèle d'épisode de soins caractérisé par la présence physique entre le soignant et le soigné dans le cadre d'un « colloque singulier », se substitue au moins partiellement une relation en continu de collecte et d'échanges d'information. Dès lors que la circulation de l'information en réseau vient compléter ou carrément remplacer l'échange en face à face, il est prévisible que des enjeux inédits se pointent, que la normativité pré-existante se trouve prise en défaut. En plus, la normativité technique impose ou induit des modalités nouvelles à la relation de soins.

Les *niveaux variables de maîtrise des outils* et environnements connectés constitue un autre ensemble d'enjeux et de risques associés aux environnements de e-santé

Bref, les environnements de e-santé font en sorte que les enjeux et risques associés à la circulation de l'information doivent être envisagés en considérant que les interactions prennent place dans un réseau et non dans des espaces physiques isolés les uns des autres.

Il ne s'agit plus seulement de l'espace de la clinique envisagé comme lieu physique contrôlé et sécurisé mais de l'environnement dans lequel sont captées des informations. L'appréhension des enjeux et risques doit aller plus loin que de simplement énumérer les obligations des professionnels et les droits des patients.

Les environnements connectés sont régis par une pluralité de normativités. Au premier chef, les normativités imposées par les configurations techniques se proposent comme constituant les premières normes, les contraintes inhérentes aux relations qui prennent place dans ces environnements. Les normativités techniques induisent des états de fait de même que les risques qui vont avec.

Il en découle un ensemble de conditions qui pourront accentuer ou minimiser les risques juridiques, ceux qui concernent la conformité aux lois et autres règles d'origine étatique.

Pour rendre compte des enjeux et des risques découlant de ces normativités, il faut analyser les environnements dans lesquels sont produites et circulent les informations.

1.2 L'évaluation des risques et des enjeux

Pour analyser les enjeux et les risques d'un environnement interactif d'information comme les PGHD, il faut procéder à l'identification des situations présentant des risques découlant de l'environnement d'information au plan des divers droits et valeurs concernés.

On identifie, à partir des situations typiques, les gisements et les flux d'informations, ce qui présente des risques de détournement d'information, puis on évalue les précautions prises ou envisageables. Une telle démarche permet de tenir compte des situations présentant des risques devant être pris en charge et de fournir les précautions nécessaires.

1.2.1 Analyser les caractéristiques de l'environnement d'information

Les interactions dans les ESP engendrent des enjeux et risques qu'il importe d'identifier afin de les gérer.

La virtualisation emporte des changements de rationalités et le défi de la gouvernance des réseaux est de procurer des méthodologies et approches optimales afin de débattre de ces enjeux et risques et formuler des modes de fonctionnement des services offrant des solutions adéquates.

Le développement des services en ligne a donc amené les entités publiques à mettre en place divers outils afin de mieux identifier les approches les plus indiquées afin d'assurer, dans les réseaux, l'identification et la maîtrise adéquate des risques et enjeux.

La première étape consiste à identifier les traits caractéristiques du fonctionnement, de la configuration et des fonctionnalités du système de e-santé envisagé afin d'y faire apparaître les enjeux que cela pose au regard des droits et obligations des personnes concernées. Cette démarche s'effectue à partir des descriptions existantes de l'environnement de e-santé.

1.2.2 Identifier les gisements et les mouvements d'information

On cerne ensuite les divers gisements d'information de même que les mouvements prévus ou envisagés de l'information personnelle qui s'effectuent dans le système. Une telle identification tient compte du cycle entier de l'information personnelle depuis sa confection, le cas échéant, sa collecte, sa détention, sa gestion, sa circulation, son utilisation, son archivage et sa destruction. Le cycle de l'information peut varier selon les types d'environnements.

Des gisements d'information sont constitués par exemple, par l'information sur les appareils connectés ou implantés chez le patient. L'information sur les appareils en possession du patient constitue aussi un gisement d'information. Il en est de même de l'information hébergée chez le fournisseur et de l'information dans les systèmes de la clinique.

Les mouvements d'information entre les différents points du réseau constituent l'autre composante de l'analyse.

On peut alors dresser un bilan des enjeux et risques soulevés à l'égard de chacune des étapes du cheminement de l'information au sein des environnements de même qu'au moment de l'entrée et de la sortie des données. Ce bilan reflète une analyse des zones de risques et de conflits.

1.2.3 Situer les responsabilités

Les enjeux et les risques ne découlent pas que de l'environnement informationnel mis en place. La responsabilité des acteurs est un relais de normativité important et un mécanisme majeur des processus de gouvernance. Il faudra situer les responsabilités des divers intervenants et décideurs oeuvrant dans les environnements cliniques. Si les questions de responsabilité doivent s'appréhender dès la conception d'un réseau, elles ne doivent pas faire oublier que les acteurs participant à ce réseau ont des rôles, des besoins et des priorités spécifiques engendrant différents niveaux et types de responsabilité.

Par conséquent, il faudra établir quel type de responsabilité correspond à chacun des acteurs, et ce pour les différents gisements et mouvements d'information. Par la suite, il faut déterminer quels outils de droit formel et informel, législatifs et contractuels, encadrent ces responsabilités au regard de la

gouvernance de l'environnement-réseau concerné, par exemple : lois et règlements, code de conduite, code d'éthique, de déontologie professionnelle, etc.

Une fois les risques et enjeux identifiés, il faut identifier méthodiquement les processus, outils et autres moyens d'expression de la gouvernance. Ces moyens doivent refléter la diversité et la complexité des réseaux et procurer des outils conceptuels afin de mettre en place des processus effectifs de gouvernance. De tels processus doivent être conséquents avec les risques et enjeux qui sont spécifiques à chacun des environnements.

Dans le secteur des soins de santé, l'analyse des enjeux relatifs à la mise en place de prestations électroniques de services peut présenter des différences avec celle qui peut être menée dans le secteur commercial[19]. Une entreprise commerciale pourra évaluer les risques associés à la mise en place de services virtualisés en termes de pertes financières. Cette évaluation est nécessaire : une entreprise peut être poursuivie devant les tribunaux et tenue responsable pour la façon incorrecte dont ses services sont offerts.

Les professionnels de la santé doivent se soucier aussi bien des conséquences financières que des conséquences non financières de leur activité. L'évaluation des risques reliés aux services offerts en ligne ne peut procéder uniquement d'une analyse des dimensions financières de l'activité concernée ou du service.

Dans l'analyse des risques, il faut tenir compte des enjeux associés au champ d'activité, de la sensibilité des informations ou des services qui sont en cause et des attentes des clientèles spécifiques.

Ces facteurs incitent généralement plusieurs entités de service public à adopter des standards qui tiennent compte des attentes du public, et pas seulement des risques spécifiques associés aux transactions.

Dans le domaine des soins de santé, il paraît indéniable qu'il faut également prendre en considération les caractéristiques inhérentes à la relation de soins.

1.2.4 Évaluer les mesures de prise en charge des enjeux et risques

La gouvernance dans les environnements de PGHD et l'ESP résulte des faits et gestes des différents acteurs. Elle se crée par des individus à travers des entités sociales et juridiques et selon des processus relationnels complexes découlant de la nature de l'espace où ils se tiennent. La normativité y est en continuelle mutation; elle résulte d'un dialogue continu entre les différents acteurs agissant dans le réseau. Il importe donc de cerner les modes de fonctionnement des réseaux dans l'ensemble des dimensions ayant des impacts sur les normes effectivement appliquées. Dans les réseaux de e-santé, le paradigme de la gouvernance permet de rendre compte d'un environnement normatif diversifié et moins formel que celui tracé par le droit étatique et formaliste. Dans une logique de gouvernance caractéristique des réseaux, la décision résulte habituellement d'une négociation permanente entre les acteurs, constitués en partenariat au sein de l'entreprise, de l'État, d'une organisation, ou même d'un problème à résoudre.

Dans les réseaux, les processus de gouvernance concernent forcément l'évaluation continue des enjeux et des risques de même que les façons de prendre en charge et de gérer les risques et enjeux.

---

19 Voir : Jane Kaufman WINN, « The Hedgehog and the Fox : Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions », [1999] 51 : *Administrative Law Review*, 955, 959-960.

2. L'environnement réseau de l'espace santé personnel

Comme mentionné, l'espace santé TELUS est une plate-forme certifiée et sécurisée, qui permet à l'utilisateur d'emmagasiner des renseignements de santé en ligne et d'en permettre le partage avec des applications ou d'autres utilisateurs autorisés.

La plate-forme s'inscrit dans la mouvance des innovations que constituent les dossiers électroniques de santé et les systèmes de partage d'information de santé. Ofir Ben-Assuli expliquent que : « The healthcare sector uses electronic technologies for medical information storage, treatment tools, medical decision making, and links between providers. »[20]

Compte tenu de sa vocation, l'espace santé TELUS fait partie d'un environnement constitué principalement des ressources informationnelles consignées dans le « Dossier santé du Québec » (DSQ) et le dossier médical électronique (DME).

L'espace santé s'inscrit dans l'écologie informationnelle de la clinique et du système de santé. Il convient de distinguer les différents ensembles informationnels qui constituent l'environnement dans lequel s'insère l'espace santé.

À l'interface entre les soignants, le patient et la clinique, l'espace santé constitue un espace de communication qui complète le dossier médical électronique (DME) et le Dossier santé Québec (DSQ).

Ces ensembles d'information doivent toutefois être situés les uns par rapport aux autres composantes de l'environnement informationnel qui est caractéristique de l'organisation contemporaine des soins de santé. Car tous ces ensembles constituent des informations rattachées au dossier du patient.

L'ESP procure les facilités afin d'interconnecter le dossier médical électronique, en émergence dans un nombre croissant de milieux cliniques et le Dossier santé Québec, qui compile et rend disponible certains ensembles de données relatives à la santé des personnes.

Il est donc opportun d'expliquer les principales caractéristiques du DSQ et du DME afin de mieux apprécier la place occupée par l'espace santé dans l'environnement informationnel de la clinique.

2.1 Le dossier médical électronique (DME)

La notion de « dossier médical électronique » renvoie fondamentalement à celle de dossier médical. Selon Inforoute santé Canada :

> *Un dossier médical électronique (DME) est un dossier médical informatisé se rattachant à un clinicien (ex. un médecin), un cabinet ou une organisation. C'est le dossier dans lequel les cliniciens consignent les données sur leurs propres patients telles que les renseignements sociodémographiques, les antécédents médicaux, le profil pharmaceutique et les diagnostics (résultats de laboratoire et d'imagerie diagnostique). Il*

[20] Ofir BEN-ASSULI, « Electronic health reords, adoption, quality of care, legal and privacy issues in their implementation in emergency departments », (2015) 119 *Health Policy* 287-297, p. 287.

> *est souvent intégré à d'autres logiciels servant à gérer d'autres fonctions telles que la facturation et la gestion des rendez-vous.*[21]

Le dossier médical électronique est le dossier du patient. Ses caractéristiques sont les mêmes que celles du dossier médical sur support papier. Les auteurs Philips-Nootens, Lesage-Jarjoura et Kouri expliquent que :

> *Le dossier du patient représente un outil indispensable pour la pratique médicale, un instrument privilégié de gestion des soins touchant tout autant la planification, l'organisation, la direction et l'évaluation. Il permet la documentation du problème de santé; il constitue une source importante de renseignements utiles dans la communication entre professionnels de la santé ou organismes intéressés, assurant ainsi la continuité de soins; il représente un élément de protection juridique; il sert à la recherche et l'enseignement.*[22]

Ils ajoutent que « le dossier médical » est indissociable de l'exercice de la médecine, car il témoigne de l'état du patient, de l'évolution de la maladie et de la conduite du médecin.[23]

Dans les environnements en réseaux, le dossier « électronique » constitue un ou plusieurs « documents »; la *Loi concernant le cadre juridique des technologies de l'information*[24], utilise le vocable « document technologique » pour désigner les documents sur des supports utilisant l'une ou l'autre des technologies capables de produire un objet dans lequel l'information est délimitée, structurée et intelligible sous la forme de mots, de sons ou d'images.

Au sens de la *Loi concernant le cadre juridique des technologies de l'information* un document tel un dossier médical électronique est constitué d'information portée par un support (art. 3). L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.[25]

De même, est assimilée à un document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Dans l'univers en réseau, il n'est pas rare que les pages apparaissant à l'écran d'un ordinateur et constituant un document sont en fait constituées d'éléments d'information physiquement conservés dans une pluralité de banques de données.

Un document constitué de signes, qu'il soit sur un support numérique ou sur un support optique, est un document technologique. Par exemple, un film sur un ruban vidéo ou sur un DVD, un fichier

---

21 INFOROUTE SANTÉ DU CANADA, *Dossiers médicaux électroniques (DME)*, en ligne : https://www.infoway-inforoute.ca/fr/accueil/85-nos-partenaires/fournisseurs/services-de-certification/269-dossiers-medicaux-electroniques-dme , consulté le 19 janvier 2106.

22 Suzanne PHILIPS-NOOTENS, Pauline LESAGE-JARJOURA et Robert P.KOURI, *Éléments de responsabilité civile médicale – Le droit dans le quotidien de la médecine*, 3e édition, Éditions Yvon Blais, 2007, no. 429

23 Suzanne PHILIPS-NOOTENS, Pauline LESAGE-JARJOURA et Robert P.KOURI, *Éléments de responsabilité civile médicale – Le droit dans le quotidien de la médecine*, 3e édition, Éditions Yvon Blais, 2007, no. 429.

24 *Loi concernant le cadre juridique des technologies de l'information,* R.L.R.Q, c. C-1.1.

25 Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012, pp. 29 et ss.

d'images sur un CD, un texte sur une disquette. Cette catégorie englobe aussi les documents multimédias.

Par contre, une conversation orale, qui n'est fixée nulle part, ne constitue pas un document. Mais elle constitue un document dès lors qu'elle est captée et fixée sur un support.

Un dossier réfère à un ensemble de documents relativement à une personne ou à une question spécifique. La notion renvoie à un ensemble de documents de même qu'au contenant de ces documents.

En vertu des règles s'appliquant à toute personne qui tient un dossier de même que selon les exigences spécifiques incombant aux professionnels de la santé, la tenue du dossier médical électronique est encadrée par différentes obligations qui s'appliquent aux différentes étapes du cycle de vie du dossier.

Le dossier doit être maintenu dans son intégralité durant tout son cycle de vie. La création du dossier, les éventuels transferts de supports, sa consultation, sa transmission, sa conservation, y compris son archivage sont tous assortis d'exigences du maintien de l'intégrité de l'information à toutes les étapes de son cycle de vie.

Car l'obligation de conserver un document emporte le devoir d'en assurer l'intégrité. Lorsqu'un document technologique est modifié durant la période pendant laquelle il doit être conservé, des conditions doivent être respectées afin d'en préserver l'intégrité en dépit de la modification (art. 21).

L'intégrité d'un document technologique doit, entre autres, être préservée dans un contexte où la garde du document est confiée à un prestataire de services. Celui-ci doit prendre les moyens technologiques convenus pour ce faire.

Lorsqu'un document est transmis, ce doit être par un mode de transmission permettant de préserver l'intégrité, tant du document expédié que de celui qui est reçu.

Des mesures de sécurité doivent protéger le dossier tout au long de son cycle de vie.

La protection des renseignements personnels et confidentiels doit être assurée à chaque phase du cycle de vie du dossier, notamment lors de sa conservation, lors de sa consultation et lors de la transmission de documents.

2.2 Le Dossier Santé Québec (DSQ)

Le DSQ est un environnement technologique hautement sécurisé qui permet de collecter, de conserver et de consulter certains renseignements de santé. Il est à la disposition des médecins et des autres professionnels de la santé du Québec. Il permet de voir, sur un écran d'ordinateur, des informations provenant de six domaines cliniques constituant des banques de données regroupant des renseignements de santé.

La *Loi concernant le partage de certains renseignements de santé*[26] identifie les personnes pouvant être autorisées à consulter les renseignements collectés par le DSQ.

Il s'agit des médecins, infirmières, pharmaciens, sages-femmes, archivistes médicales, les biochimistes, infirmières auxiliaires, microbiologistes, résidents et stagiaires en médecine et en

[26] R.L.R.Q., c. P-9.0001.

pharmacie ainsi que les personnes qui agissent en soutien technique auprès des médecins et des pharmaciens.

Ces personnes doivent obtenir des droits d'accès les autorisant à consulter le DSQ.

Les droits d'accès identifient les renseignements qui peuvent être consultés. Ces droits sont établis par le *Règlement sur les autorisations d'accès et la durée d'utilisation des renseignements contenus dans une banque de renseignements de santé d'un domaine clinique*, règlement édicté par le ministre de la santé[27].

Les renseignements collectés et conservés dans le DSQ ne peuvent être utilisés que par des personnes autorisées et uniquement dans le cadre d'une prestation de soins ou de services de santé.

Lors d'une consultation, un professionnel de la santé peut ajouter un renseignement obtenu du DSQ dans le dossier médical électronique d'une personne. Les règles de confidentialité applicables au dossier médical électronique assurent la protection de ce renseignement. À l'instar de tous les autres renseignements consignés dans le dossier médical, ces informations ne peuvent être communiquées à d'autres personnes sans le consentement du patient concerné, sauf dans les situations d'exception prévues par la loi.

L'article 11 de la *Loi concernant le partage de certains renseignements de santé* habilite le ministre à constituer six domaines cliniques qui sont :

> *1° le domaine médicament;*
>
> *2° le domaine laboratoire;*
>
> *3° le domaine imagerie médicale;*
>
> *4° le domaine immunisation;*
>
> *5° le domaine allergie et intolérance;*
>
> *6° le domaine sommaire d'hospitalisation.*

Un domaine clinique se compose d'une ou de plusieurs banques de renseignements de santé.

À ce jour, les trois derniers domaines ne sont pas encore en vigueur.

Certaines personnes autorisées ont accès à une partie seulement des renseignements collectés par le DSQ, alors que d'autres ont accès à la totalité de ces renseignements.

Des mesures rigoureuses de sécurité, dont des mécanismes d'accès sécurisés, sont en place afin d'assurer la confidentialité des renseignements collectés par le DSQ.

Ainsi, avant de pouvoir transmettre des renseignements de santé concernant un patient ou de consulter le DSQ, les personnes autorisées doivent obtenir des droits d'accès auprès de la Régie de l'assurance maladie et se soumettre à un processus rigoureux de vérification de l'identité afin de recevoir un dispositif d'accès. En plus, les personnes accédant au DSQ doivent utiliser un poste de travail spécialement configuré à cette fin et s'authentifier au système à l'aide d'un dispositif de sécurité

---

[27] R.L.R.Q., c. P-9.0001, r. 1.

et d'un mot de passe personnel. De plus, l'authentification doit être réitérée régulièrement, puisque l'utilisateur est débranché automatiquement après une certaine période d'inactivité.

Tous les professionnels de la santé sont soumis à un code de déontologie qui les oblige à respecter la vie privée de leurs patients et à assurer la confidentialité des renseignements contenus dans leurs dossiers. Le code de déontologie régissant chaque professionnel habilité à accéder aux renseignements du DSQ est applicable.

Le DSQ est régi par un ensemble de règles très strictes en matière de confidentialité et de respect de la vie privée. De lourdes sanctions sont prévues pour les personnes qui contreviendraient à ces règles.

Chaque fois que des personnes autorisées consultent les renseignements concernant un patient ou ajoutent de nouveaux renseignements, leur signature électronique et l'action réalisée s'enregistrent automatiquement. L'accès aux renseignements de santé d'une personne dans le DSQ laisse donc nécessairement une trace afin de garantir la confidentialité et de permettre un recours en cas d'infraction.

Chaque personne inscrite au DSQ a le droit d'obtenir, sur demande, la liste des personnes qui ont accédé à ses renseignements. Elle doit à cette fin faire une demande au responsable de l'accès des documents et de la protection des renseignements personnels du Ministère de la santé. La demande doit obligatoirement être accompagnée d'une copie d'une preuve d'identité valide avec photo et signature.

Si un renseignement concernant un patient est erroné, incomplet ou équivoque, celui-ci a le droit d'en demander la correction auprès du responsable de l'accès des documents et de la protection des renseignements personnels.

Même avec consentement, les renseignements du DSQ concernant un patient ne peuvent être transmis à un assureur ou un employeur ou à une personne qui exerce une fonction dans le domaine du contrôle ou de l'expertise, par exemple, un médecin de la Société de l'assurance automobile du Québec (SAAQ) ou de la Commission de la santé et de la sécurité du travail (CSST) ou à quiconque, dans le but de conclure un contrat exigeant l'évaluation de l'état de santé d'une personne.

C'est donc dire que toute personne qui travaille dans le réseau de la santé et qui exerce une fonction d'expertise ou de contrôle auprès d'un assureur (par exemple : Société de l'assurance automobile du Québec, Commission de la santé et de la sécurité du travail) n'est pas autorisée, dans le cadre de cette fonction, à consulter les renseignements qui sont consignés dans le DSQ.

Ainsi, hormis ces interdictions prévues par la réglementation régissant le DSQ, des mouvements d'information entre le DSQ et le DME sont possibles.

Une fois dans le DME, les renseignements issus du DSQ font partie du dossier médical de la personne et peuvent, moyennant consentement de celle-ci, être communiqués à d'autres personnes, par exemple, au moyen de la plate-forme espace santé TELUS

2.3 Les caractéristiques générales de l'espace santé TELUS

Une vaste gamme de renseignements de santé d'une personne peuvent être stockés et partagés grâce à cette «plate-forme de partage de données en ligne» qu'est l'espace santé TELUS et on peut y accéder par de multiples applications et appareils afin d'en prendre connaissance

Par exemple, le projet espace santé personnel de la clinique Nouvelle Beauce est une application branchée à l'espace santé TELUS qui permet de rassembler, de stocker et d'organiser les renseignements de santé du patient dans un dossier unique centralisé. Le patient ou son représentant autorisé peut consulter les données de son dossier de santé tel que contenu sur la plate-forme sécurisée de l'Espace Santé TELUS grâce au portail patient. L'équipe clinique autorisée (agent administratif, infirmière auxiliaire, infirmière GMF) peut consulter l'espace santé personnel via le portail clinicien.

Pour utiliser l'espace santé TELUS, l'utilisateur doit ouvrir un **compte** auquel il accède par un ensemble d'authentifiants. L'utilisateur peut créer un **dossier** pour lui et pour les membres de sa famille. Lorsqu'il crée un dossier, l'utilisateur en devient le gestionnaire, qui est le niveau d'accès sécurisé le plus élevé qui donne le contrôle absolu du dossier.

En tant que gestionnaire d'un dossier, il peut alors **partager** les renseignements de santé du dossier (en tout ou en partie) avec des tiers (parents ou amis), des fournisseurs de soins de santé ou des applications logicielles (par exemple lorsque ces applications ajoutent des données au dossier de la personne, fournissent des renseignements au fournisseur de soins de santé de la personne ou utilisent les données inscrites dans certains dossiers de santé de la personne pour lui donner des conseils sur les façons de gérer sa santé). Et personne ne peut accéder au dossier tant que le gestionnaire n'a pas indiqué clairement sa décision de le partager ou de permettre d'y accéder.

En plus de pouvoir partager le dossier, le gestionnaire peut aussi y ajouter ou supprimer des renseignements de santé, visualiser l'historique des changements apportés au dossier et même supprimer le dossier.

Le gestionnaire d'un dossier peut aussi inviter de nouveaux utilisateurs à devenir gestionnaire de son dossier et d'autres utilisateurs peuvent l'inviter à devenir gestionnaire du leur. Chaque gestionnaire peut ajouter et supprimer des gestionnaires ainsi que les utilisateurs qui peuvent consulter et modifier le dossier.

Un compte peut regrouper les dossiers de santé de plusieurs personnes, l'utilisateur et les membres de sa famille, mais il est établi au nom d'une seule personne, l'utilisateur. Et chaque dossier contient les renseignements sur une seule personne. Et un dossier peut compter plusieurs gestionnaires.

2.3.1 Les composantes de l'espace santé

L'espace santé est constitué d'un espace privatif personnel au titulaire participant. Celui-ci peut autoriser d'autres personnes à accéder à ses informations. La plate-forme permet aussi de réaliser des échanges de documents dans un cadre sécurisé et authentifié.

2.3.1.1 L'espace sécurisé personnel

L'espace santé personnel est un service de traitement et de conservation de « documents technologiques », c'est-à-dire des documents élaborés grâce au recours aux technologies de l'information, ce qui inclut les documents numériques[28].

C'est un espace sécurisé doté de fonctions d'encryptage et d'horodatage. C'est un espace virtuel de stockage et de conservation de documents sécurisé et permettant de restituer ce qui y a été déposé.

---

[28] *Loi concernant le cadre juridique des technologies de l'information*, R.L.R.Q. c C-1.1, art. 3. http://canlii.ca/t/q5zn. Voir Pierre Trudel, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012, 29-43.

Il permet d'entreposer des documents comportant des renseignements sur la situation de santé de la personne.

Selon la *Loi concernant le cadre juridique des technologies de l'information*[29], cela implique que l'environnement possède les différentes fonctions permettant de dire que les documents qui s'y trouvent ou qui en émanent sont intègres au sens de la loi.

Au sens de la loi, la notion de documents technologiques désigne des documents qui sont sur un support faisant appel aux technologies de l'information qu'elles soient électroniques, magnétiques, optiques, sans fil ou autres ou une combinaison de plusieurs technologies.

Les données constitutives des documents que l'utilisateur y dépose sont en fait traitées de manière à ce qu'il soit possible de retrouver les documents dans leur intégralité. Il est de même possible de documenter les différents évènements relatifs à chacun des documents traités dans le système. Le tout permet de disposer de documents technologiques dont l'intégrité est assurée.

Les documents technologiques qui sont déposés sont nécessairement authentifiés et horodatés. Ces caractéristiques permettent d'affirmer, si le traitement est effectué conformément aux conditions, que les documents traités dans le contexte de l'espace santé personnel sont intègres au sens de la Loi. Selon la loi québécoise, un document est intègre si, suivant le support utilisé, la stabilité et la pérennité de l'information sont assurées, et s'il est possible de vérifier que l'information n'est pas altérée et qu'elle est maintenue dans son intégralité[30]. Alors, de tels documents ont pleine valeur juridique et peuvent éventuellement être produits en preuve devant les tribunaux.

Les caractéristiques de cet environnement électronique doivent permettre d'effectuer une telle vérification.

2.3.1.2 L'espace des échanges

Il est possible de transmettre des documents, en expédier ou en recevoir au moyen de la plate-forme espace santé TELUS. Le document technologique reçu aura la même valeur que le document transmis car la transmission dans la plate-forme permet de préserver l'intégrité des deux documents et, comme cela est exigé par la Loi, la documentation établissant la capacité du mode de transmission utilisé dans la plate-forme est disponible pour production en preuve, le cas échéant. L'ensemble des échanges dans l'espace santé s'effectue en mode sécurisé et crypté, ce qui permet de s'assurer de la plus stricte confidentialité des échanges.

Aussi, tous les dépôts de documents technologiques dans l'espace santé personnel se font de manière à garantir l'intégrité des documents dans le temps.

Il existe également une fonction d'horodatage (date et heure certaine) et de scellement par signature électronique afin d'archiver légalement des documents technologiques.

Ainsi, le document qui est issu de cet espace utilisé conformément aux spécifications est intègre au sens de la loi.

Le système fonctionne grâce à l'utilisation d'un identifiant et d'un mot de passe qui permet à l'usager d'accéder au système. Ce processus actionne notamment les certificats. Or, l'usager, aussi bien le

---

29 *Loi concernant le cadre juridique des technologies de l'information*, R.L.R.Q. c C-1.1, <http://canlii.ca/t/q5zn>.

30 *Loi concernant le cadre juridique des technologies de l'information*, article 6.

professionnel ou autre membre de l'équipe soignante et les patients - ont l'obligation de protéger les certificats et les données d'identification qui y donnent accès.

La possibilité de faire passer du DSQ au DME puis du DME à l'espace santé emporte les possibilités de transferts d'informations du DME et du DSQ. Compte tenu des règles strictes régissant le DSQ, prohibant l'accès à certaines catégories de personnes, il est certain que l'usage de l'espace santé présente un risque manifeste de priver d'effet pratique les interdictions relatives aux informations consignées dans le DSQ. De même les renseignements en provenance du DME se retrouvant dans l'espace santé d'une personne pourraient se trouver à la disposition de personnes qui n'ont pas en principe droit d'accès au DSQ ou au DME.

Il s'agit ici d'un risque inhérent à l'espace santé dans la mesure où on y verse des informations provenant des deux autres répertoires que sont le DSQ et le DME. L'utilisateur de l'espace santé, qui doit évidemment exprimer son consentement, doit être bien au fait des enjeux inhérents à une telle possibilité de partage d'information.

2.3.2 Les gisements d'information de l'espace santé personnel

Dans l'espace santé personnel, les gisements d'information sont constitués de documents que l'usager décide lui-même de consigner dans son espace mais pour l'essentiel, il s'agit d'informations provenant de la clinique. Il ne s'agit pas pour l'heure de données dynamiques, dotées de liens logiques et structurés de façon à être transmis.

Mais il y a aussi des gisements d'information constitués lors de la vérification de l'identité de l'usager effectuée lors de l'inscription de même que les informations collectées et conservées afin d'assurer le bon fonctionnement de l'infrastructure à clé publique (ICP) qui y est associée.

Il y a les données qui sont en possession du fournisseur de service afin de valider l'identité d'une personne qui se présente afin d'accéder à l'espace.

Toutes ces données doivent évidemment être conservées intègres et sécurisées à un degré conséquent avec le niveau de confiance associé à cet espace. Le lieu physique dans lequel sont entreposés les données est situé au Canada ou est sous le contrôle d'une entité canadienne.

Compte tenu des exigences de certaines lois sur les soins de santé, il pourra être nécessaire de déterminer que les lieux physiques dans lesquels sont consignés les données sont bien situés au Canada.

Toutes les informations contenues dans l'espace santé personnel comportent une **indication de la provenance**. Par exemple, dans le projet de la clinique Nouvelle-Beauce, un code couleur permet de distinguer la source (Bleu pâle : information ajoutée ou modifiée par l'utilisateur lui-même par le portail patient ; Orange : information ajoutée ou modifiée par le personnel de la clinique par le portail clinicien ; Gris : information transmise par la clinique ou bien par un dispositif connecté comme un glycomètre)

2.3.2.1 Les données saisies par l'utilisateur avec le portail patient

- Pour accéder à son espace, l'utilisateur introduit son identifiant puis introduit son code secret. Par la suite, une fois identifié dans le système, il sera loisible au participant d'ajouter, modifier ou supprimer son information démographique, les personnes à contacter en cas d'urgence, période de temps cible, unités de mesures préférées, saisir manuellement des données de glycémie ou de tension d'appareils non compatibles avec

espace santé TELUS, ajouter de données concernant les médicaments. Il peut inscrire les rendez-vous, notes et questions qu'il veut aborder avec l'équipe de soins lors de son prochain rendez-vous.

2.3.2.2 Les données transférées par le médecin et l'équipe de soins

- Pour accéder au portail, le professionnel inscrit son nom d'utilisateur et son mot de passe. Il n'a accès qu'à la liste des patients qui lui ont donné accès à leur espace santé personnel. Accès aux données du patient : En cliquant sur le nom du patient, il peut accéder à ses données détaillées et a une vue complète de son espace santé personnel : Conditions/antécédents, informations médicales, poids, diabète, cardio, rendez-vous, messages, suivis de santé. Journal santé, Questionnaires et documents, information patient, rapport.

- Lorsque le DME géré dans KinLogix est connecté à l'espace santé personnel, le médecin ou le professionnel, avec le consentement du médecin, peut effectuer le transfert des données aux patients du DME KinLogix à l'espace santé personnel du patient.

- Des données médicales **sélectionnées** par le **médecin** de l'utilisateur sont **transférées** à l'ESP de l'utilisateur : ex. allergies, intolérances, signes vitaux (tension artérielle, pouls), médicaments, poids, taille, résultats de tests laboratoire signés et autres documents en format PDF.

- L'équipe de soins peut envoyer un plan de soins que l'utilisateur doit suivre ou des questionnaires afin de faire le bilan de son état de santé (suivi du diabète, de l'hypertension, TDAH, journal de santé). [31]

- L'infirmière clinicienne assure le transfert des données pertinentes au médecin. Le médecin pourra consulter les données transférées par l'infirmière et pourra transférer des données au patient si nécessaire. Au suivi clinique du patient, le médecin génère les données pertinentes dans le DMÉ qui seront ensuite transmises à l'espace santé personnel si jugé nécessaire et pertinent par le médecin. [32]

- La tâche de transférer les données médicales peut être attribuée à un autre membre de l'équipe au nom du médecin avec son consentement. Pour ce qui est des tests de laboratoire la même procédure que pour une version papier s'applique : le rapport doit être vu par le médecin et signé avant d'être transmis.

- Le médecin ou la personne autorisée conserve en tout temps un contrôle sur l'information qu'elle transfère grâce aux options de partage qu'elle peut cocher directement dans son DME à l'intérieur de la note clinique.

2.3.2.3 Les données transmises par les appareils médicaux en ligne

- Les informations provenant des appareils médicaux et de condition physique en ligne tels tensiomètres, lecteurs de glycémie, pèse-personnes, oxymètres, pédomètres, appareils de

---

31 *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 35.

32 TELUS, *Espace santé TELUS, Spécifications fonctionnelles-Centre médical de la Nouvelle Beauce*, version 1.1, october 10, 2014, p. 8 et 9.

mesure de pointe DEP) peuvent être envoyées vers le compte espace santé personnel de l'utilisateur avec le logiciel gratuit *HealthVault Connection Center* [33].

- Lorsque l'utilisateur connecte son appareil médical à son ordinateur, le *HealthVault Connection Center* envoie les données qu'il contient vers le dossier Espace santé Telus de l'utilisateur, qui sont enregistrées sous l'onglet «Mes mesures»

Cette configuration implique des enjeux et risques relatifs aux gisements d'information.

Des enjeux découlent des lieux où sont stockées les données : est-ce qu'elles sont conservés dans l'appareil médical ou sur le *cloud* du prestataire de services? Si, elles sont entreposées dans l'infonuage, il importe d'évaluer la durée et les conditions de cet entreposage.

D'autres questions nécessitent aussi des réponses : les données peuvent-elles être détruites et comment? Par le patient? Que fait le prestataire avec ces données? (les vendra-t'il? Peut-il les utiliser à sa discrétion pour adapter sa publicité? Peut-on les produire sous ordre de la cour?).

Voilà autant d'enjeux soulevés par ces gisements d'information.

2.3.3 Les mouvements d'information : le partage des données médicales dans l'espace santé personnel

L'utilisateur peut partager ses informations médicales avec une personne de confiance, et lui permettre de consulter, d'utiliser, de mettre à jour ou de supprimer des informations, selon le niveau d'accès qu'il lui accorde.

Par exemple, il peut utiliser le partage afin de fournir à une personne ses informations médicales essentielles en cas de situation d'urgence, de laisser un enfant adulte, une personne soignante, un fournisseur de soins surveiller sa santé, de partager le dossier d'immunisation d'un enfant ou de partager des renseignements sur sa condition physique avec un entraîneur personnel.

En plus de les imprimer, de les exporter ou de les enregistrer, l'utilisateur peut partager ses informations médicales de plusieurs façons : en accordant à une personne l'accès à une partie ou à la totalité de son dossier de santé; en désignant un opérateur avec plein accès aux données et en désignant un fournisseur de soins. Pour utiliser un outil médical en ligne, il doit nécessairement l'autoriser à accéder à ses informations médicales.

2.3.3.1 En accordant à une personne l'accès à une partie ou à la totalité de son dossier de santé

L'utilisateur peut inviter une autre personne à accéder aux données de son espace personnel ou de celui de tout autre personne dont il est opérateur par l'envoi d'une invitation à partage (par ex. : à un parent, à un professeur pour lui permettre d'accéder au dossier d'un enfant afin de compléter des questionnaires d'évaluation etc). Pour ce faire, la procédure est la suivante : inscription du destinataire à l'espace santé personnel, création d'un code secret pour s'assurer que seul le destinataire pourra accéder à l'invitation de partage, niveau de partage (afficher seulement, afficher et modifier, opérateur) et catégorie d'informations désirée et date d'expiration des droits d'accès[34]. Le

---

[33] *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 29 et 33.

[34] Voir *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, pp. 21-23.

courriel d'invitation au partage contient un lien vers une page sur laquelle la personne peut accepter ou refuser la demande de partage et celle-ci doit posséder son propre compte espace santé personnel[35].

L'utilisateur peut accéder à tous les profils autorisés de son compte (ex : membres de la famille) et basculer d'un profil à l'autre. Cela facilite la gestion des informations médicales de la famille. Si plusieurs personnes veulent accéder au dossier d'une autre personne et l'utiliser (ex : deux personnes gèrent la santé d'un parent âgé en perte d'autonomie), l'une d'elles doit créer un dossier pour le parent pour ensuite le partager avec l'autre personne[36].

Par contre, en cas de modifications des relations familiales ou autres, se soulèvent des enjeux quant à la discontinuation des droits d'accès à l'espace santé par exemple, par un ancien conjoint ou par une personne à laquelle le titulaire de l'ESP souhaite retirer les droits qu'elle s'était vue conférer sur son espace santé

Dans le cas d'un parent invitant un tiers à partager le dossier de son enfant, certaines questions se posent : qu'arrive-t'il lorsqu'un adolescent devient, généralement lorsqu'il atteint l'âge de quatorze ans, apte à gérer son propre dossier?

Des interrogations similaires se posent à l'égard de tiers, par exemple, un entraîneur dans le cadre d'un programme de conditionnement physique ou un professionnel de la santé qui cesse de soigner le titulaire de l'ESP.

Il importe de prévoir un ensemble de mesures et précautions lorsque prend fin une relation ou une situation familiale ou parentale fondant le droit d'une personne d'accéder à un espace santé d'une personne.

2.3.3.2 En désignant un opérateur

C'est une personne qui a le plein accès à toutes les informations d'un dossier espace santé TELUS, de telle sorte qu'elle peut consulter, modifier, ajouter, partager et supprimer n'importe laquelle de ces informations. Les opérateurs peuvent consulter les informations marquées comme personnelles par d'autres utilisateurs et ils peuvent voir l'historique de toutes les modifications effectuées dans le dossier, y compris les articles supprimés dans la corbeille d'espace santé TELUS. Les opérateurs peuvent supprimer définitivement des informations du dossier.

Il faut choisir soigneusement les personnes à qui on accorde un accès à titre d'opérateur, car elles auront le plein contrôle du dossier, y compris la capacité d'annuler l'accès de l'utilisateur à ce dossier. L'utilisateur qui accorde un tel statut à une personne doit être bien informé des conséquences de ce geste.

2.3.3.3 En désignant un fournisseur de soins

C'est le professionnel de la santé qui suit l'état de santé de l'utilisateur et qui lui propose des plans de suivis de santé contenant des tâches ainsi que des objectifs précis. Il peut également lui envoyer des questionnaires afin d'obtenir davantage d'informations sur son état de santé. Par défaut, dans le

---

35 *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, pp. 27.

36 *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, pp. 27.

projet pilote, c'est le Centre médical de la Nouvelle Beauce. Ceci permet au personnel du centre médical d'avoir accès à l'information médicale et aux données de journalisation et de suivi que l'utilisateur inscrit dans son espace santé personnel. Cette démarche nécessite une simple autorisation directement par le ESP lors de l'inscription[37].

2.3.3.4 Accès par l'outil médical en ligne au dossier de l'utilisateur

Pour utiliser un outil médical en ligne avec espace santé TELUS, l'utilisateur doit d'abord l'autoriser à accéder à ses informations dans son espace santé TELUS[38].

En effet, un outil médical peut devoir consulter, ajouter, mettre à jour ou supprimer des informations contenues dans le dossier de l'utilisateur qui sont liées aux tâches qu'il accomplit. L'utilisateur peut annuler à tout moment l'accès d'un outil médical en ligne. L'utilisateur peut connaître les modifications apportées à son espace santé personnel en consultant l'historique dans le portail patient.

Cependant, l'annulation de l'accès d'un outil médical au dossier Espace santé TELUS ne supprime pas toutes les informations contenues dans cet outil.

Se pose également la question de ce qu'il advient des informations collectées à partir de l'outil médical connecté à un ESP. Ces risques sont habituellement divulgués au niveau de l'outil médical connecté mais il subsiste la question de l'effet cumulatif du raccordement de l'ESP à un ensemble d'outils médicaux connectés. La question du traitement des informations recueillies à partir des outils médicaux et conservés par les serveurs associés à de tels outils se pose aussi. Des risques significatifs de circulation d'information et de perte de confidentialité doivent ici être pris en considération.

2.4 Les enjeux généraux de l'espace santé personnel

Différents enjeux et risques doivent être examinés à l'égard des évènements qui surviendront tout au long du cycle d'utilisation de la plate-forme. D'une façon générale, l'espace santé personnel décrit ici soulève des enjeux similaires à ceux des systèmes de données générées par les patients (Patient-Generated Health Data, PGHD)[39].

2.4.1 L'inscription et l'accès à l'espace santé personnel

L'inscription constitue habituellement une étape cruciale dans la détermination des niveaux de précautions qui sont requis compte tenu des enjeux associés à l'environnement informationnel envisagé.

La vérification de l'identité, l'authentification du patient ou du médecin qui inscrit de l'information est essentielle afin d'assurer que cette information est attribuée à lui ou elle avec confiance. Un mécanisme liant l'information à sa source est important afin de suivre l'information dans le système,

---

37 TELUS, *Espace santé TELUS, Spécifications fonctionnelles-Centre médical de la Nouvelle Beauce*, version 1.1, october 10, 2014, pp. 13-14.

38 Voir *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 31.

39 Voir National eHealth Collaborative, *Patient-Generated Health Information-Technical Expert Panel*, Final Report, December 2013; Office of the National Coordinator for Health Information Technology, Issue Brief : Patient-Generated Health Data and Health IT, December 20, 2013; M. Shapiro, D. Johnston, J. Wald et D. Mon, Patient-Generated Health Data, White Paper, April 2012.

particulièrement lorsque l'information est partagée, et d'assurer son intégrité. Si le patient ne veut pas que les données soient partagées avec d'autres fournisseurs ou pour d'autres buts, il faut obtenir son autorisation pour un partage secondaire des données. Il faut bien établir l'identité du personnel qui reçoit et accède à l'information et s'assurer qu'il est bien autorisé. La transmission de l'information doit être sécuritaire et l'encryptage, nécessaire.

2.4.2 Les données médicales contenues dans l'espace santé personnel

2.4.2.1 Sécurité et caractère confidentiel des informations

Afin d'évaluer les enjeux et risques à cet égard, il importe d'obtenir des précisions sur les questions suivantes :

Par exemple, qu'en est-il du caractère confidentiel des documents qui y sont consignés, de même que les limites qui sont prévues par la Loi à l'égard de la confidentialité?

À quelles conditions un document consigné dans cet environnement peut-il être utilisé dans le cadre de transactions? etc.

Qu'en est-il de la sécurité des renseignements?

Quelles sont les caractéristiques des lieux dans lesquels les données sont reçues et entreposés?

2.4.2.2 Préoccupations techniques

Les données doivent être recueillies et soumises d'une façon standardisée afin de s'assurer qu'elles seront non seulement reçues mais aussi comprises et intégrées dans le dossier du patient. Un vocabulaire facilement compréhensible doit être utilisé pour le portail patient afin d'aider le patient à soumettre l'information pertinente et utile.

2.4.3 Le partage des données médicales

Il importe de valider le processus par lequel s'effectue le partage des données médicales.

2.4.3.1 Communication et délai de transfert des données

Des enjeux importants concernent la communication des informations entre le patient et le médecin. Est-ce que les données envoyées ont été enregistrées dans le dossier? Comment le patient est-il informé que le médecin ou l'équipe de soins a reçu l'information qu'il lui a transmis?

Est-ce qu'il existe un mécanisme de notification signalant que quelqu'un l'a vue? Comme nous le verrons plus en détail dans la partie consacrée aux responsabilités des soignants et de la clinique, il importe de préciser entre l'usager et les professionnels concernés, les conditions dans lesquelles les informations versées dans l'ESP sont effectivement vues et considérées par le professionnel de la santé.

Il faut prévoir des réponses à des questions telles que :quand le médecin verra l'information? Aujourd'hui? Le patient recevra-t-il une réponse? Quand? Les données fournies par le patient ont-elles été tenues compte et bien reçues par le médecin? L'une des préoccupations d'un patient est de savoir si le médecin ou l'équipe de soins a bien reçu ou vu les données qu'il a envoyées et s'il confirmera la réception.

Qu'en est-il du délai de transfert des données? Le délai de transfert des données vers le compte de l'utilisateur varie selon le médecin puisque c'est lui qui doit examiner les données devant être transférées, certains transferts exigeant plus de temps que d'autres. Des risques réels au regard de la responsabilité du médecin pour l'information qui n'a pas été revue à temps et celle qui requiert une réponse urgente doivent être considérés et donner lieu à une ligne de conduite claire et raisonnable.

2.4.3.2 Flux continu d'information et responsabilité

La relation de soins peut se trouver passablement métamorphosée par le flux continu d'information. Pour le médecin, le grand flux d'information peut-il interférer avec son habileté à fournir des soins de qualité? Le médecin a-t-il besoin de connaître toutes les mesures de glucose et autres? Comme le médecin a le fardeau de revoir un grand nombre de données médicales, sa responsabilité est-elle augmentée? (Préoccupations quant au *Too much data)*

Quant au patient, est-ce que ses attentes sont réalistes?

Le fait que le médecin soit engagé dans une relation de soins plus continue augmente-t'il sa responsabilité? Le fait de ne pas avoir revu les données médicales qui lui ont été envoyées ou de ne pas avoir agi à temps suivant ces données peut-il engager sa responsabilité pour des événements qui était auparavant en-dehors du processus de soins mais qui en font désormais partie? Un médecin pourrait-il être tenu responsable pour une décision basée sur des données non reçues à temps, s'il manque des données essentielles pour prendre une décision, si le dossier contient des erreurs de données ou si les données ne sont plus utiles au moment où elles sont reçues par le médecin? Les données correspondent-elles au bon patient? La source des données est-elle disponible ou digne de confiance?

L'impact financier des PGHD et des espaces santé personnels est difficile à déterminer tant qu'on ne sait pas comment ils s'intègreront dans l'ensemble des modèles de soins existants. S'il y a une charge de travail additionnelle pour un médecin de revoir les données, y a-t'il un impact financier dans un environnement où il est payé au volume? Quels sont les impacts possibles sur la productivité?

Les conditions de succès des PGHD et ESP dépendent des attentes qui doivent réalistes et bien comprises. Les médecins et les patients doivent avoir une compréhension commune sur les données qui ont de la valeur, sur la façon dont elles sont partagées et sur ce qui arrive après que les données sont partagées. Sinon, des attentes irréalistes et non partagées risquent de conduire à des conséquences non désirées pour les patients et les médecins. Lorsque les fonctionnalités des PGHD et ESP sont bien implantées, incluant un ensemble de politiques et de procédures pour s'assurer de la transparence quant à l'utilisation des données du patient, les préoccupations et la responsabilité potentielle diminuent.

Il y a ici un important enjeu quant aux conditions du déroulement de telles interactions prenant place dans un tel espace de communication.

Il paraît évident que les modes de pratique fondés sur des épisodes de rencontres fixés dans le temps ne sont pas automatiquement compatibles avec un mode de partage d'information qui se déroulerait en continu. La consultation médicale opère actuellement selon un modèle supposant le partage d'information entre le patient et le professionnel de la santé dans le cadre d'une rencontre située dans le temps et dans l'espace.

Avec l'espace santé, on est en présence d'un modèle de flot continu d'information; le recours à l'espace santé pour échanger des informations en flots continus suppose donc une modification majeure de la structure de la relation entre le soignant et le patient.

Un tel enjeu paraît accentué avec le développement et la généralisation prévue des outils connectés de télémesure capables de produire et de pousser des informations en temps réel.

2.4.3.3 Partage secondaire des données

Les données sont-elles partagées avec l'assureur du patient? Avec ses parents, conjoint, partenaire? Le partage a-t'il été fait de façon appropriée? Les données ont-elles utilisées pour la recherche clinique ou à d'autres utilisations secondaires? Dans l'affirmative, les risques associés à l'ESP sont significativement accrus.

2.4.3.4 Fin de l'utilisation de la plate-forme

L'utilisation de la plate-forme peut prendre fin volontairement lorsque l'utilisateur décide de ne plus en faire usage. Se pose alors la question des modalités de récupération des documents qu'il y avait placés.

La fin de l'utilisation peut découler du décès ou de l'incapacité de l'utilisateur. Alors se pose la question des conditions auxquelles les représentants légaux de l'utilisateur peuvent y accéder et disposer des documents et renseignements qui s'y trouvent.

Une fois fermé, l'utilisateur dispose d'une période de grâce de 90 jours durant laquelle il peut demander que son compte espace santé TELUS soit ré-ouvert et ses données restaurées. Après ces 90 jours, toutes les informations stockées dans le compte de l'utilisateur seront définitivement supprimées, sauf si d'autres opérateurs ont accès à des dossiers dans le compte de l'utilisateur. Dans ce cas, l'utilisateur en est averti au moment de fermer son compte et ces dossiers ne seront pas supprimés.

On recommande à l'utilisateur d'exporter et d'enregistrer ses informations avant de supprimer son compte.[40]

[40] Voir *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 9.

3. Le cycle de fonctionnement de l'espace santé personnel

L'espace santé personnel rendu possible grâce à la plate-forme TELUS permet de gérer un ou plusieurs dossiers de santé, ceux créés pour la personne elle-même ou les membres de sa famille et ceux dont elle est gestionnaire. Un compte peut regrouper les dossiers de santé personnels de plusieurs personnes, mais il est établi au nom d'une seule personne. Chaque dossier contient les informations médicales d'une seule personne. Il peut être géré et partagé indépendamment des autres dossiers, ce qui permet de conserver les informations de chaque personne séparément.[41]

Lorsqu'une personne crée un dossier, elle en devient gestionnaire, c'est-à-dire le niveau d'accès sécurisé le plus élevé qui donne le contrôle absolu du dossier incluant la possibilité d'ajouter et de supprimer des renseignements de santé.

En se fondant sur le cycle d'utilisation de l'espace santé par les participants, ce chapitre passe en revue les enjeux et risques qui sont associés à chacune des étapes, en commençant par le processus d'ouverture d'un compte, jusqu'à la fin de l'utilisation de l'espace santé, en passant par le dépôt et le traitement de documents. On y explique les principes généraux applicables aux documents qui sont consignés dans l'espace santé personnel. Un tel environnement contient nécessairement des documents technologiques et présente des caractéristiques pouvant avoir des conséquences sur le caractère confidentiel des renseignements de santé que les utilisateurs y consignent.

Cela permet de décrire les dispositions applicables de la législation québécoise lors des différentes situations relatives à un document se trouvant dans un tel environnement ou qui est utilisé dans le cadre d'échanges et de transactions.

3.1 L'ouverture d'un compte utilisateur

L'ouverture du compte d'utilisateur, c'est-à-dire le processus au terme duquel un citoyen devient un participant à l'expérience pilote de l'espace santé personnel, comporte les étapes suivantes :

- préinscription en clinique
- création d'un compte espace santé TELUS
- transfert des données du DMÉ
- sélection de l'équipe de soins
- inscription d'un membre de la famille ou d'une autre personne au compte Espace santé TELUS
- acceptation des termes et conditions
- activation du compte

[41] Voir *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 6.

3.1.1 Les étapes de l'inscription à l'espace santé personnel

3.1.1.1 Préinscription en clinique et inscription à la maison

- La préinscription s'effectue à la clinique. L'agent administratif sélectionne le patient à inscrire à partir du DMÉ-Kinlogix .

- Le patient sélectionne une question de sécurité et l'agent inscrit la réponse ainsi que l'adresse courriel du patient. Ce mot de passe sera utilisé comme authentifiant lors de la réception de l'inscription à la maison.

- L'agent transmet l'invitation à s'inscrire au patient par courriel.

- La préinscription terminée, le patient pourra compléter son inscription chez lui

- De retour chez lui, le patient ouvre le courriel qui contient l'invitation à s'inscrire à l'espace santé personnel, clique sur le lien «Inscription à l'ESP» et répond à la question secrète déterminée lors de sa visite à la clinique. Pour connecter à l'espace santé personnel, il faut créer un compte espace santé TELUS.

3.1.1.2 Création du compte espace santé TELUS

- Pour ouvrir une session sur espace santé TELUS, il faut saisir un nom d'utilisateur et un mot de passe. Espace santé TELUS accepte l'identificateur Windows Live. Lorsqu'on ouvre une session à l'aide de l'identificateur Windows Live, Espace Santé TELUS se sert de l'adresse courriel et du mot de passe associé à cet identificateur.

- En ouvrant une première session, la première étape pour accéder à un espace santé personnel (comme celui des projets Nouvelle Beauce ou d'Angus) est de créer un compte sur espace santé TELUS.

- Pour créer un compte, la personne doit fournir des renseignements personnels tel son nom, sa date de naissance, son adresse courriel, son code postal et son pays ou sa région. Ces renseignements sont obligatoires; d'autres renseignements peuvent être demandés mais ils sont facultatifs.

- Elle confirme les renseignements de son compte, procède à l'acceptation des conditions d'utilisation de TELUS Microsoft. Le compte espace santé TELUS est maintenant créé.

- TELUS enverra une demande de confirmation d'adresse courriel à l'adresse inscrite afin d'inscrire cette dernière dans les invitations à partage que la personne enverra au moyen de l'Espace santé TELUS. L'adresse courriel peut également être utilisée par les fournisseurs d'appareils médicaux (ex : podomètre, glycomètre, tensiomètre artériel) et d'applications (outil de gestion de maladies chroniques ou application d'entraînement physique, de perte de poids ou de pression artérielle) suivant leur politique relative à la protection des renseignements personnels.

- La personne peut alors procéder à la création de dossiers pour elle-même ou pour les membres de sa famille ou autre, à condition dans ce dernier cas, d'obtenir les consentements nécessaires.

- La création et l'ouverture d'un compte comporte des enjeux et risques relativement à l'identification et l'authentification.

3.1.1.3 Transfert des données du DMÉ

- Le patient doit autoriser les applications (Kinlogix et Espace santé personnel de la clinique) à accéder à ses informations médicales dans l'Espace santé TELUS en sélectionnant son dossier et en cliquant sur «Autorisez l'accès ». Il y a transfert des données de la clinique au dossier.

3.1.1.4 Sélection de l'équipe de soins

- Le patient doit également autoriser le personnel clinique à accéder à son dossier en sélectionnant le praticien dans son ESP pour permettre les communications et l'accès de l'équipe clinique au dossier du patient par l'interface clinique du ESP. Le clinicien est alors autorisé à accéder à son dossier et à communiquer avec le patient par le ESP. Cette démarche nécessite une simple autorisation directement dans l'ESP. Le personnel clinique peut ainsi avoir accès à l'information médicale et aux données de journalisation et de suivi que le patient inscrit dans son DSP. Cette opération s'effectue automatiquement.

3.1.1.5 Inscription d'un membre de la famille ou d'une autre personne au compte espace santé TELUS

- Lors de l'inscription, l'utilisateur peut ajouter plus d'un profil (dossier) à un même compte et basculer d'un profil à l'autre, et gérer ainsi la santé de plusieurs membres de sa famille. Il n'y a pas de limite au nombre de personnes dont on peut conserver le dossier dans son compte espace santé personnel[42].

- L'utilisateur doit avoir une invitation en provenance du Centre médical de Nouvelle Beauce pour ajouter une nouvelle personne à son compte espace santé TELUS, que ce soit les membres de sa famille ou tout autre personne. Une fois l'invitation en main, l'utilisateur peut compléter l'inscription et ajouter le dossier à son compte.

- Par exemple, pour *l'inscription d'un enfant par le parent*, le parent reçoit le courriel qui contient l'invitation pour la connexion au dossier de l'enfant aux données en provenance du DMÉ et l'accès à l'application du ESP. À partir de son propre compte, le parent autorise ensuite les deux applications (soit le DMÉ et l'ESP) à accéder au dossier de l'enfant. Une fois l'autorisation en place, le DMÉ est autorisé à téléverser des données au dossier de l'enfant en tout temps. Le parent peut donc consulter les données transmises par l'équipe clinique au moyen du ESP.

- Il y a des enjeux associés au fait que des proches peuvent accéder à l'espace santé d'un patient, parents pour leurs enfants, accès des personnes aidantes (aidants naturels)

3.1.1.6 Acceptation des termes et conditions

- Comme mentionné, lors du premier accès à l'ESP, le patient doit accepter les termes et conditions d'utilisation et le consentement se fait dans un formulaire en ligne et est conservé en mémoire et cette opération n'est requise qu'une seule fois :

> *«Le contenu de l'Espace santé Personnel est fourni à titre informatif et ne doit pas être interprété comme étant un avis médical.*

---

42 *Guide de l'utilisateur*, Espace santé personnel, Centre médical de la Nouvelle Beauce, version 3.0, 9 avril 2015, p. 29.

Le centre médical de La Nouvelle Beauce ne garantit aucunement que l'information déposée dans l'espace Santé sera consultée par le personnel de la clinique ou par les médecins.

En cas de besoin, veuillez communiquer directement avec votre clinique ou appeler le 9-1-1»

- Ce message d'avertissement est aussi affiché en continu sur la page d'accueil du portail patient et visible à chaque connexion par le patient[43].

- L'inscription est terminée.

- Une fois qu'il a reçu son identifiant et son mot de passe, le participant se trouve titulaire d'un espace sur la plate-forme. À compter de ce moment, la plupart de ses droits et obligations sont définis par la relation contractuelle qui s'est établie dans le contrat d'utilisation.

3.1.2 La vérification d'identité lors de l'inscription

L'inscription suppose d'établir avec un niveau élevé de certitude, l'identité de chacun des participants. Les exigences applicables au processus de confirmation de l'identité des personnes sont énoncées à l'article 40 de la *Loi concernant le cadre juridique des technologies de l'information.*

La vérification d'identité est effectuée par une personne relevant de la clinique et chargée par celle-ci de la vérification d'identité (agent vérificateur).

L'inscription d'une personne pour la mise en fonction d'un identifiant ou d'un compte d'identité électronique doit se faire auprès d'une personne qui présente de sérieuses garanties de fiabilité.

Dans le modèle retenu, TELUS assume les tâches de gestion des clés et des certificats de même que de l'infrastructure opérationnelle. Et les fonctions de vérification d'identité sont assumées par la clinique lors de l'inscription. Une fois le processus d'inscription complété, il y a uniquement une relation entre la clinique et le patient.

Ces tâches supposent l'identification du participant et l'attribution des identifiants.

Dans le schéma envisagé lors de l'étude, la clinique assume les fonctions de vérification d'identité. Ces fonctions concernent les opérations suivantes :

- Confirmer l'identité des participants en obtenant de leur part les pièces justificatives qui correspondent au niveau de certitude requis, compte tenu du niveau de sécurité conséquent avec les enjeux associés au projet ;
- Valider que la personne est habilitée à détenir les droits et qualités qui seront mentionnés dans le certificat ;
- Initier le processus de génération des clés du participant ;
- Initier le processus de génération des certificats des participants ;
- Recevoir et traiter les demandes de révocation, de suspension ou de réactivation des certificats.

---

43 TELUS, *Espace santé TELUS, Spécifications fonctionnelles-Centre médical de la Nouvelle Beauce*, version 1.1, october 10, 2014, p. 16.

Le risque assumé par l'autorité responsable de l'inscription– ici la clinique - est particulièrement important puisqu'elle est «le tout premier maillon du processus qui permet de passer d'une situation concrète concernant une personne à une situation virtuelle d'identification et d'octroi de "droits".»[44]

Étant donné qu'une fois émis, le certificat devient « infalsifiable » en termes cryptographiques puisqu'il est signé par la clé privée de l'autorité émettrice du certificat, cette phase de vérification d'identité est cruciale. C'est en effet au cours de cette étape que le risque de fraude est élevé puisque c'est à ce moment qu'il est possible pour une personne d'obtenir un certificat en se faisant passer pour une autre personne.

C'est pourquoi les procédures d'identification mises en place par l'autorité responsable de l'inscription doivent refléter l'ampleur du risque acceptable et accepté. Par exemple, la présence physique de la personne et la présentation de pièces d'identité procurent un niveau plus élevé de certitude quant à l'identité de la personne alors que l'identification en ligne, c'est-à-dire, sans avoir vu la personne peut présenter des garanties moindres quant à la certitude.

En assumant la fonction de vérification de l'identité des participants, la clinique a une importante responsabilité face aux participants, aux citoyens qui seraient victimes de fraude (par une personne venant se faire passer pour eux lors du processus d'identification), face au gestionnaire des clés et des certificats de même qu'à l'égard de tous les partenaires qui pourraient subir des dommages en raison de fraude ou autres gestes fautifs commis au moment de la phase d'identification.

Dans un tel processus, l'établissement de la confiance est primordial entre les partenaires se trouvant en communication, que ce soit avant, pendant ou après l'échange. Avant l'échange, les partenaires doivent obtenir la garantie que l'interlocuteur à l'autre bout de la ligne est celui qu'il prétend être (authentification). Pendant l'échange, le récepteur du message veut s'assurer que le message qu'il reçoit est bien celui que son correspondant a envoyé (intégrité) ou que l'échange soit confidentiel (confidentialité). Et enfin, après l'échange, les partenaires veulent une garantie que la participation à l'échange ne sera pas niée par une partie (non-répudiation).

Avant d'émettre un certificat, l'autorité de certification (AC), ici TELUS, doit s'assurer de l'identité de la personne qui détiendra les clés et le certificat. Pour ce faire, elle doit recueillir un certain nombre de renseignements personnels relatifs à cette personne.

À cette étape du processus de vérification d'identité, les **gisements et les mouvements de renseignements personnels** sont les suivants:

- Les renseignements personnels collectés par l'agent vérificateur d'identité (ici la clinique) sont ceux figurant dans les pièces d'identité présentées par chaque participant.
- Les renseignements personnels tels les références aux pièces vérifiées.
- Les renseignements personnels transférés de l'agent vérificateur d'identité à l'ICP (infrastructure à clé publique) sont le compte-rendu de la vérification d'identité au service de certification signifiant ainsi la demande de délivrance du certificat pour le participant.

Les risques sont ici de la même nature que ceux qui existent lorsqu'une personne confie des informations à un professionnel. Dans des infrastructures à clé publique de niveau comparable, comme le Registre des droits personnels et réels mobiliers du Québec (RDPRM), les agents vérificateurs d'identité sont des professionnels, comme les notaires, ils sont régis par un code de déontologie. Pour les notaires, ce code les oblige au secret professionnel. La clinique pourrait confier

44 Thierry AUTRET, Laurent BELLEFIN et Marie-Laure OBLE-LAFFAIRE, *Sécuriser ses échanges électroniques avec une PKI-Solutions techniques et aspects juridiques*, Paris, Éditions Eyrolles, 2002, p. 216.

cette tâche à des membres de son personnel exerçant des fonctions qui les situent à un niveau élevé de confiance.

3.1.2.1 Les qualités des personnes effectuant la vérification de l'identité

Dans un tel projet, c'est la clinique qui a la responsabilité de confirmer l'identité du citoyen en obtenant des pièces justificatives. Il lui revient de vérifier qu'une personne a bien l'identité, les droits et la qualité qui seront indiqués dans le certificat. Les qualités que doivent posséder les membres du personnel de la clinique qui seront chargés de la vérification de l'identité des participants est un enjeu important.

En effet, l'autorité qui prend en charge l'inscription a la responsabilité de tâches relatives à la gestion des demandeurs et de leurs certificats, entre autres celle de confirmer l'identité du demandeur en obtenant des pièces justificatives à la constitution et à l'exploitation du certificat, de valider s'il est habilité à obtenir les droits ou qualités mentionnés dans le certificat, d'obtenir la clé publique du demandeur de l'entité responsable, de vérifier que le demandeur est en possession de la clé privée associée à la clé publique pour laquelle il demande un certificat et de soumettre les demandes de génération de certificat vers l'émetteur de certificat[45].

Les contrôles, c'est-à-dire l'authentification du demandeur et la vérification de ses attributs par l'autorité d'enregistrement (AE, ici la clinique), lui confèrent un droit de transiger dans l'espace santé. Les auteurs Autret, Bellefin et Oble-Laffaire écrivent à cet égard qu':

> *En effet, une fois qu'il est généré le certificat devient infalsifiable en termes cryptographiques puisqu'il est signé par la clé privée de l'AC* [autorité de certification]. *C'est donc pendant cette phase que peuvent se passer les fraudes visant à obtenir un certificat à la place de quelqu'un d'autre. C'est pour cette raison que des responsabilités importantes reposent sur l'AE et ses agents d'enregistrement, et qu'il est rare de déléguer cette fonction à des sous-traitants.*[46]

Des enjeux majeurs doivent être considérés au regard des agents chargés de rencontrer et d'identifier les personnes qui participeront au système. Ces agents ont la lourde responsabilité d'établir si une personne est suffisamment identifiée pour qu'on puisse considérer que l'on a la certitude nécessaire pour prendre pour acquis que la personne qui présentera le certificat qui lui sera remis pourra effectivement être considérée comme étant cette personne. Et cela sans que les autres personnes impliquées dans le fonctionnement de l'espace santé aient vu cette personne.

Compte tenu du fait que le système a vocation à conserver et échanger des documents technologiques qui seront tenus pour être authentiques, signés et opposables, il faut que la vérification initiale d'identité procure des garanties élevées quant à l'identité des personnes. C'est dire l'importance de l'opération par laquelle un agent d'identification rencontre le participant, examine ses pièces d'identité et dresse un compte-rendu de sa démarche.

3.1.2.2 La collecte d'information identifiante

À l'instar de toute utilisation d'information portant sur des personnes, la vérification de l'identité doit se faire dans le respect de la loi.

---

45 Thierry AUTRET, Laurent BELLEFIN et Marie-Laure OBLE-LAFFAIRE, *Sécuriser ses échanges électroniques avec une PKI-Solutions techniques et aspects juridiques*, Paris, Éditions Eyrolles, 2002, p. 44.

46 Thierry AUTRET, Laurent BELLEFIN et Marie-Laure OBLE-LAFFAIRE, *Sécuriser ses échanges électroniques avec une PKI-Solutions techniques et aspects juridiques*, Paris, Éditions Eyrolles, 2002, p. 44.

À l'égard des prestations électroniques de services assumés par l'État, la nécessité de l'information identifiante s'apprécie en fonction du contexte spécifique de chaque type de prestation. Il y a une obligation de proportionnalité entre, d'une part, les besoins de certitude qui doivent être satisfaits par l'identification et, d'autre part, le principe de retenue dans la collecte d'information personnelle. Afin de décider de manière adéquate des mécanismes et processus d'identification dans un environnement de transactions électroniques, il faut se poser un ensemble de questions et y apporter des réponses dans l'ordre approprié. C'est là une première fonction de l'analyse des risques et enjeux[47].

Or, dans le cas présent, le système à être mis en place suppose un niveau élevé de sécurité car les documents concernés seront authentiques et opposables. Il faut s'assurer que les possibilités qu'une personne se fasse passer pour une titulaire de compte dans le système soient proches de zéro.

La pratique dans les infrastructures à clé publique de niveau de sécurité comparable à celui qui est ici envisagé est d'effectuer la vérification de l'identité uniquement en face à face avec la personne participante.

Lorsque la demande pour une carte ou un compte d'identité électronique est faite en personne, l'identité de l'individu va généralement être vérifiée en examinant deux pièces d'identité ou des copies certifiées de ces pièces, un code client ou un code de vérification confidentiel, ou des copies certifiées d'autres documents tel le certificat de naissance.

La pratique observée à l'égard de prestations comportant des niveaux de risques comparables à celle du présent projet est de demander, lors de l'identification, deux pièces d'identité dont une avec photo.

Dans toutes les situations, il importe que la personne qui procède à l'identification soit convaincue de l'identité de la personne. Si, dans le cadre d'une expérience pilote, il peut être tout à fait raisonnable de s'en remettre aux connaissances des préposés de la clinique pour vérifier l'identité, le déploiement à grande échelle de l'ESP nécessite des précautions comme celles que nous décrivons ici, compte tenu du niveau d'enjeux et de risques qui sont ici impliqués.

La clinique joue le rôle de «facilitateur». Les ordinateurs utilisés au moment de l'inscription servent à collecter les informations nécessaires et à les transmettre à TELUS qui conserve ces informations sur ses serveurs. Les informations collectées ne doivent pas être croisées avec d'autres bases de données.

3.1.2.3 Les fonctions de gestion des clés et des certificats

TELUS est l'entité qui émet les certificats et génère à partir de ses systèmes, les clés des utilisateurs. La clinique effectue la vérification de l'identité des participants. Une fois effectuée la vérification de l'identité, un responsable de la clinique transmet des documents attestant de l'identité du participant et enclenche le processus technique par lequel sont mis en service les identifiants, soit les clés et certificats du participant.

Dans le contexte de l'espace santé, différents aspects relatifs à l'identification devraient être formalisés dans l'hypothèse d'un déploiement à grande échelle. Ainsi, il faudra déterminer si la seule la carte d'assurance maladie constitue un élément suffisant pour établir l'identité d'un usager.

---

47 Pierre TRUDEL et France ABRAN, *Guide sur la mise en place et l'administration de mécanismes d'identification électroniques,* préparé pour le Secrétariat du Conseil du Trésor, Québec, avril 2001, < http://www.chairelrwilson.ca/guides/guideB.html >.

Il faudra identifier avec précision les obligations de la clinique lors de la remise du mot de passe et assurer l'information du participant à l'égard de ses identifiants, codes et carte, mots de passe.

En particulier, il importe de prévenir le participant des conséquences qu'il pourrait subir s'il laisse une autre personne utiliser sa carte ou son mot de passe.

Lors de la remise de l'identifiant (codes et carte, mots de passe), la clinique doit informer le participant de ses obligations à leur égard. Cet identifiant active les clés et les certificats permettant d'initier des transactions qui auront des conséquences juridiques pour lui ou pour d'autres.

Les obligations du participant sont précisées aux articles 57 et 58 de la *Loi concernant le cadre juridique des technologies de l'information*. Le titulaire d'un certificat doit s'assurer que le dispositif ne soit pas utilisé sans autorisation. Il doit en assurer la confidentialité, notamment en conservant secrets les codes (NIP) associés à son identifiant.

Le participant doit être expressément prévenu qu'il lui incombe de voir à ce que son identifiant (la Loi vise « le dispositif ») ne soit pas utilisée sans autorisation. Toute utilisation est présumée faite par lui.

Le participant a donc la responsabilité de prendre les mesures adéquates afin que sa clé privée, par exemple, qui lui est attribuée, ne soit pas accessible à d'autres. En effet, un individu ne pourrait se plaindre des conséquences d'une usurpation d'identité s'il laisse d'autres personnes, par exemple, utiliser sa carte comportant un certificat équivalant à sa signature. La loi crée même une présomption d'utilisation par le titulaire. Il devra donc en cas d'usurpation prouver que c'est quelqu'un d'autre qui a utilisé sa clé privée, le cas échéant, ce qui peut s'avérer assez difficile.

L'article 57 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit, *a contrario*, que le dispositif peut être utilisé par une autre personne avec l'autorisation du titulaire : par exemple lorsqu'une société signe par l'intermédiaire de l'un de ses employés ou dirigeants, elle doit prendre les moyens pour s'assurer que c'est bien cet employé ou ce dirigeant qui signera en son nom, puisque toute utilisation est présumée faite par cette société.

La clinique, en tant que responsable de l'inscription a aussi sa part de responsabilité, car lors de la remise au titulaire de l'élément secret du dispositif, elle doit prendre les moyens qui s'imposent pour que ce soit seulement le titulaire visé qui en prenne connaissance et le reçoive (art. 57).

S'il a des motifs raisonnables de croire que son certificat a été perdu ou autrement compromis, le participant a l'obligation d'aviser tous ceux qui peuvent être affectés par cette perte. En effet, l'article 58 prévoit les obligations du titulaire d'un dispositif, dans le cas où celui-ci a été volé ou perdu ou lorsque des données confidentielles ont été compromises. Il doit aviser, dans les meilleurs délais :

1° la personne qu'il a autorisée à utiliser le dispositif ;

2° le tiers dont il peut raisonnablement croire qu'il agit en se fondant sur le fait que le dispositif a été utilisé par la personne qui en a le droit ;

3° le prestataire de services de certification pour que ceux-ci puissent suspendre ou annuler le certificat lié à la carte.

L'expression «qui a des motifs raisonnable de croire» est assez exigeante: le participant doit aviser les personnes visées même s'il n'est pas certain que son certificat a été perdu ou compromis. Il doit le faire aussitôt qu'il a un soupçon sérieux à cet égard.

Le participant a aussi l'obligation de mise à jour des renseignements fournis en vue de l'obtention de son certificat et ce dans les meilleurs délais (art. 59).

L'utilisation de tablettes ou de téléphones intelligents sera éventuellement possible pour accéder à l'espace santé personnel. Il faudra alors envisager les modalités différentes d'accès, les conditions ou les accès conséquents.

3.2 L'utilisation par le participant

Dans la présente partie, l'on identifie et évalue les risques et les enjeux de l'espace santé personnel aux principales phases de son cycle d'utilisation.

On y passe en revue les processus associés à l'utilisation de l'espace santé personnel en signalant les risques associés à chacun des évènements du cycle de l'information: le dépôt, l'entreposage, la modification, l'échange et le partage d'un document. On examine les mouvements d'information et les utilisations possibles de celle-ci, qu'est-ce qu'il advient de l'information transmise par l'utilisateur, comment est-elle traitée, conservée et partagée, etc.

Compte tenu des caractéristiques de l'espace santé personnel, il importe de déterminer avec précision « qui » contrôle cet espace et à quel degré, le patient, la clinique ou un partenaire ? L'identification du contrôle en tout ou en partie de cet espace permet de définir et répartir les responsabilités de chacun. Lorsqu'on s'interroge sur les responsabilités, on se demande qui est tenu de répondre des situations problématiques qui se manifestent.

Les risques doivent donc être appréciés à la lumière des caractéristiques que présentent les différentes composantes de l'environnement espace santé. Le système sera analysé en fonction des droits et obligations des participants. Ces droits et obligations seront identifiés en fonction des phases du cycle de vie des documents technologiques.

Le participant a la pleine maîtrise de son espace. Il est responsable de ce qu'il décide d'y mettre. Il utilise l'espace santé personnel afin d'y déposer des documents technologiques. Les documents qui seront traités dans un tel environnement sont régis principalement par la *Loi concernant le cadre juridique des technologies de l'information*. Mais ces documents sont aussi assujettis au régime des informations de santé et du secret médical.

3.2.1 Le dépôt d'un document dans l'espace santé personnel

Le dépôt dans l'espace santé personnel peut nécessiter un transfert de support. Il pourra en effet être nécessaire de transférer le document d'un support papier à un support numérique. Un tel transfert s'effectue avant l'introduction du document dans l'espace santé personnel.

Différents types d'appareils de même que des entreprises proposent des systèmes permettant de transférer des documents sur support papier vers des documents en format numérique.

Le participant qui souhaite y placer des documents qui sont sur support papier va devoir transférer ces documents vers un support numérique afin de les déposer dans l'espace santé personnel.

Les articles 17 et 18 de la *Loi concernant le cadre juridique des technologies de l'information* traitent du processus de changement du support de l'information (par exemple : transférer une photo sur support papier vers un fichier numérique sur CD, transférer l'information contenue sur une bande sonore vers un disque CD, imprimer sur papier un document numérique…).

L'article 18 vient faciliter l'admission en preuve des documents résultant de transfert. L'article 17 traite de la question du transfert technologique couramment appelé « migration des supports » :

> ***17.*** *L'information d'un document qui doit être conservé pour constituer une preuve, qu'il s'agisse d'un original ou d'une copie, peut faire l'objet d'un transfert vers un support faisant appel à une technologie différente.*
>
> *Toutefois, sous réserve de l'article 20, pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur juridique, le transfert doit être documenté de sorte qu'il puisse être démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée.*
>
> *La documentation comporte au moins la mention du format d'origine du document dont l'information fait l'objet du transfert, du procédé de transfert utilisé ainsi que des garanties qu'il est censé offrir, selon les indications fournies avec le produit, quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert.*

La condition de la validité du transfert est qu'il doit être documenté. Il faut être en mesure de démontrer, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée. C'est la condition requise afin que le document source puisse être détruit et remplacé par le document transféré tout en conservant sa valeur juridique. S'il s'agit de la destruction d'un document dont la conservation est exigée par la loi, elle doit se faire en plus suivant les exigences de l'article 20.

Le contenu minimal de la documentation est précisé par le troisième alinéa de l'article 17. Elle doit comporter la mention du format d'origine du document dont l'information a été transférée, du procédé de transfert utilisé, et des garanties que ce procédé est censé offrir quant à la préservation de l'intégrité du document devant être transféré et du document résultant du transfert. Ces garanties sont celles qui figurent dans les indications fournies avec le produit utilisé.

La documentation, y compris celle relative à tout transfert antérieur, est conservée durant tout le cycle de vie du document résultant du transfert. La documentation peut être jointe, directement ou par référence, soit au document résultant du transfert, soit à ses éléments structurants ou à son support.

Le dépôt d'un document dans un environnement technologique est un geste régi par l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*. Selon cette disposition, une personne qui confie un document technologique à un prestataire qui doit en assurer la garde, doit informer ce prestataire des protections que requiert le document en ce qui a trait à la confidentialité de l'information. Le prestataire est tenu d'en assurer la sécurité, d'en préserver l'intégrité et d'en protéger la confidentialité (article 26).

Dans le cas de l'espace santé personnel, la nature même du service fourni implique que les documents sont hautement sécurisés, sous le contrôle exclusif de l'utilisateur et leur confidentialité est protégée à l'égard de toute autre personne.

Une fois déposé dans l'espace santé personnel, l'intégrité du document doit être maintenue durant tout son cycle de vie pour qu'il puisse conserver sa valeur juridique[48]. La *Loi* énonce les mesures à prendre afin d'assurer le maintien de l'intégrité du document tout au long de son cycle de vie. C'est-à-dire, lors du transfert de l'information vers un autre support, lors de la conservation du document, lors de sa consultation et lors de sa transmission.

---

48 *Loi concernant le cadre juridique des technologies de l'information,* article 6, alinéa 2.

En plus d'être encrypté et horodaté, le document qui est placé dans l'espace santé personnel est associé à un identifiant qui le suivra tout au long de son cycle de vie. L'article 46 de la *Loi concernant le cadre juridique des technologies de l'information* énonce à cet égard que :

> ***46.*** *Lorsqu'un document utilisé pour effectuer une communication en réseau doit être conservé pour constituer une preuve, son identifiant doit être conservé avec lui pendant tout le cycle de vie du document par la personne qui est responsable du document.*
>
> *L'identifiant du document doit être accessible au moyen d'un service de répertoire, dont une des fonctions est de relier un identifiant à sa localisation. Le lien entre un identifiant et un objet peut être garanti par un certificat lequel est lui-même accessible au moyen d'un service de répertoire qui peut être consulté par le public.*
>
> *L'identifiant se compose d'un nom de référence distinct et non ambigu dans l'ensemble des dénominations locales où il est inscrit, ainsi que des extensions nécessaires pour joindre ce nom à des ensembles de dénominations universels.*
>
> *Pour permettre d'établir la provenance ou la destination du document à un moment déterminé, les autres objets qui ont servi à effectuer la communication, comme les certificats, les algorithmes et les serveurs d'envoi ou de réception, doivent pouvoir être identifiés et localisés, au moyen des identifiants alors attribués à chacun de ces objets.*

L'article 46 vise les documents qui doivent être conservés pour fins de preuve et prévoit la possibilité de faire cette preuve à l'aide d'identifiants. Il prescrit les exigences qui doivent être respectées lorsqu'un document est utilisé afin d'effectuer une communication sur un réseau, c'est-à-dire transmettre une information, et que ce document doit être conservé afin de pouvoir, le moment venu, en faire la preuve.

La principale exigence est que l'on doit conserver l'identifiant du document, et ce, pendant tout son cycle de vie. La personne responsable du document assume cette obligation. L'identifiant est une notion technique qui vise essentiellement le nom de référence du document et des objets qui servent à établir sa provenance ou sa destination. Pour que cette preuve puisse être faite, les identifiants doivent être inscrits dans un répertoire accessible au public.

3.2.2 L'entreposage d'un document

Lorsque le participant introduit un document dans son l'espace santé personnel, il effectue une transmission de ce document. Le document technologique est en effet transmis au serveur. Mais il n'est pas « communiqué » à l'entité qui opère le serveur ou la plate-forme. Celle-ci agit uniquement comme intermédiaire pour entreposer un document.

La communication suppose que l'information est portée à la connaissance d'une personne. Or, la plate-forme n'a aucunement connaissance de la teneur des documents que les utilisateurs mettent dans leur espace santé personnel. Cette distinction est importante car elle permet de rendre compte du fait qu'on ne songe pas à rendre responsable une entité qui ne fait que déplacer un document d'un point d'expédition à un autre point dans la mesure où elle n'acquiert pas le contrôle sur ce document. À l'instar du facteur qui livre une lettre, le fournisseur de la plate-forme a beau être en pleine possession physique des documents, il n'a pas le contrôle de ceux-ci puisqu'il n'a pas le droit d'en

prendre connaissance. Lorsqu'une personne en possession physique d'un document comportant des renseignements personnels n'a pas le droit de les utiliser, ceux-ci ne lui sont pas communiqués[49].

Par contre le fournisseur de services est tenu de conserver les documents entreposés dans les espaces santé personnels. Aux termes de l'article 19 de la *Loi concernant le cadre juridique des technologies de l'information*, il a le devoir d'en assurer l'intégrité et l'accessibilité pour ceux qui ont le droit d'y avoir accès. Il doit voir à la disponibilité du matériel permettant de le rendre accessible et de l'utiliser aux fins auxquelles il est destiné. Par exemple, il doit disposer du logiciel ou du matériel nécessaire pour que l'on puisse accéder et prendre connaissance du document.

Aux termes de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau, n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier. Ainsi, lorsque le « prestataire-intermédiaire » propose une plate-forme dans laquelle il est loisible aux usagers de commander des informations, par exemple en actionnant un lien pour ensuite les acheminer à un tiers, le prestataire qui offre de tels services de conservation n'acquiert pas le contrôle sur les documents ainsi traités. Faute de contrôle, ces documents ne lui sont pas communiqués. C'est bien davantage l'usager qui se fait communiquer des documents et décide de les transmettre à un tiers.

La communication se distingue donc de la transmission qui consiste à rendre disponible un document pour une communication. Tant que le document n'est que transmis, il n'est pas effectivement communiqué. Par contre, la transmission se présente habituellement comme une situation ayant vocation à mener à la communication du document. Mais dans l'hypothèse d'une transmission dans un espace santé personnel, l'usager ne communique pas le document à une autre personne. Il l'entrepose dans un espace sécurisé.

Par ailleurs, la plate-forme offre des possibilités de communiquer un document technologique de façon sécurisée et ce avec des garanties d'authenticité du document transmis et communiqué. La *Loi concernant le cadre juridique des technologies de l'information* prévoit des règles relatives à l'identification et à la localisation des objets, de manière à établir leur provenance ou leur destination, et ce, à l'aide d'un identifiant, qui devrait être accessible au moyen d'un service de répertoire. Comme mentionné précédemment, l'article 46 vise les documents qui doivent être conservés pour fins de preuve et prévoit la possibilité de faire cette preuve à l'aide d'identifiants. Il prescrit les exigences qui doivent être respectées lorsqu'un document est utilisé afin d'effectuer une communication sur un réseau, c'est-à-dire transmettre une information, et que ce document doit être conservé afin de pouvoir, le moment venu, en faire la preuve. La personne responsable du document doit conserver l'identifiant du document (essentiellement le nom de référence du document et des objets qui servent à établir sa provenance ou sa destination), et ce, pendant tout le cycle de vie du document.

3.2.3 La modification d'un document dans l'espace santé

Par ses fonctions, l'espace santé personnel doit permettre de respecter les conditions imposées par la législation québécoise en ce qui a trait au maintien de l'intégrité du document lorsque celui-ci est modifié. Si ces conditions n'étaient pas observées, il pourrait être considéré que la modification de l'information constitue une altération du document, ce qui lui ferait perdre son intégrité, qui fonde sa valeur juridique. Par exemple, une modification à un document consigné dans l'espace santé

[49] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 95 et suiv.

personnel sera, pour préserver l'intégrité des documents, documentée par les fonctions d'horodatage et de signature que comporte le service d'hébergement.

Dans l'ESP, les documents ne peuvent être modifiés que par celui qui les ont introduits. Ainsi, un document introduit par un médecin ne peut être modifié que par lui. Un document introduit par un patient ne peut être modifié que par lui.

Lorsqu'un document technologique est modifié, durant la période pendant laquelle il doit être conservé, des conditions doivent être respectées afin d'en préserver la valeur juridique en dépit de la modification:

> ***21.*** *Lorsqu'une modification est apportée à un document technologique durant la période où il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct.*

Sous peine de faire perdre au document sa valeur juridique, la personne qui a l'autorité pour faire la modification doit noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui ainsi que la raison de la modification. La modification ainsi effectuée fait partie intégrante du document même si elle se trouve sur un document distinct. Cela peut être dans une annexe ou son équivalent.

Dans beaucoup de situations, les métadonnées procurent les informations exigées par la Loi comme condition du maintien de l'intégrité d'un document technologique. Selon les outils logiciels utilisés pour traiter les documents et notamment pour effectuer des modifications, il pourra être possible de générer la documentation requise par l'article 21.[50] Or, les fonctions de l'espace santé personnel procurent la documentation exigée en vertu de l'article 21. Il est en effet possible de disposer d'un état documenté des modifications apportées à un document qui se trouve dans l'espace santé personnel.

3.2.4 L'échange et le partage d'un document

Les documents consignés dans l'espace santé personnel peuvent être échangés, partagés ou autrement traités avec d'autres personnes disposant d'un espace dans la plate-forme. L'espace santé personnel donne accès à des fonctions de transmission de même qu'à d'autres fonctions inhérentes aux échanges effectuées en ligne au moyen de documents technologiques.

À l'instar des autres environnements en réseaux, l'espace santé suppose des informations qui sont essentiellement circulantes, disponibles au moment où elles doivent l'être pour accomplir une prestation de soins.

Ces conditions de circulation accrue des informations nécessitent aussi des précautions car les potentialités d'accumulation et de couplage des informations sont plus considérables dans de tels réseaux que dans les échanges prenant place dans le cadre classique de la relation de soins.

Cela appelle une attitude réaliste tenant compte aussi bien des avantages de la circulation des informations que de ses inconvénients.

Dans un contexte comme celui de l'espace santé, l'enjeu n'est plus tellement de savoir si une information peut ou non être en possession d'une autre personne que celle qui est directement

---

50 David HRICIK and Chase Edward SCOTT, « Metadata : The Ghosts Haunting e-Documents, » (2009) 26 *The Computer & Internet Lawyer*, 23-34, p. 24.

concernée mais plutôt si cette dernière a le droit d'en faire usage pour prendre une décision dans une situation spécifique.

La circulation et le partage des informations permettent d'améliorer la qualité et la célérité des prestations. Les échanges et le partage de l'information permettent de limiter les situations dans lesquelles les personnes sont obligées de retransmettre les mêmes informations; on réalise des gains de productivité qui devraient globalement profiter à tous.

3.2.4.1 Le partage

Pour identifier les enjeux et risques associés aux fonctions de partage, il convient de les situer selon les principales phases du cycle de partage.

- Le partage est initié par l'attribution de permissions d'accès. Ces permissions sont-elles graduables, en fonction des différents types de documents ?

- La décision d'autoriser le partage

  C'est à la personne concernée par les informations de santé qu'il revient a priori d'autoriser le partage, donc l'accès par d'autres aux informations de santé qui sont consignées dans son espace personnel.

  Dans certains cas, c'est à une autre personne que revient la faculté d'autoriser un partage, typiquement, une personne de l'entourage qui exerce l'autorité parentale ou agit en vertu d'un mandat de protection.

  Cas des titulaires de l'autorité parentale : Les titulaires de l'autorité parentale peuvent agir au nom des personnes mineures sous leur protection.

  Se pose cependant la question du départage des droits et responsabilités lorsque la personne mineure atteint l'âge de quatorze ans puis l'âge de dix-huit ans.

  Cas des personnes mandataires pour une personne inapte ou sans être déclarée inapte, n'est pas en mesure de prendre ce type de décision.

  Que permet le partage? Il importe en effet de déterminer les personnes qui ont l'autorisation de permettre le partage des informations consignées dans l'espace santé. Normalement, il s'agit de personnes exerçant l'autorité parentale ou détentrices de mandats de protection ou en cas d'inaptitude.

- Accéder aux informations consignées dans l'espace santé

  Dans quelle mesure est-il possible de baliser le partage de renseignements ?

  Quels ajouts possibles aux renseignements? De quelle façon ces informations sont-elles validées?

  Quelles sont les informations qu'une personne autorisée à partager est en droit d'ajouter, de modifier ou de retrancher ?

  Quelles modifications possibles?

  Quelles suppressions ?

Qui est responsable du partage et donc de l'autoriser ou d'y mettre fin?

À priori, la personne qui est titulaire de l'espace santé est celle qui autorise. Elle est donc responsable de l'accès aux documents consignés. Est-ce que cette responsabilité est partagée avec d'autres ? Avec la clinique ? Peut-elle être partagée ?

Dans certains cas, il pourrait s'avérer difficile d'attribuer une information.

- Information préalable aux patients

  Il faut informer les patients des enjeux et risques spécifiques au partage.

  Dans quelle mesure les patients en position d'autoriser le partage d'informations sont-ils informés des possibilités et des modes de fonctionnement du partage?

- Le contrôle de l'usager

  L'économie générale des règles en matière de protection des renseignements personnels milite en faveur de la reconnaissance effective d'un haut niveau de maîtrise au profit des usagers concernés par les informations.

  Selon l'étude de Prasad, Sorber, Stablein, Anthony et Kotz[51], les participants valorisent la capacité de contrôler et de décider quelle information partager, avec qui et dans quelles circonstances.

  La flexibilité des outils permettant de contrôler le partage est aussi un enjeu identifié par les usagers.

- Les conditions générales des accès à un dossier (espace santé)

  La gradation des droits d'accès : en fonction des enjeux associés aux différents niveaux de permissions : Lecture seulement, Modifications possibles, Pouvoirs complets

En somme, les enjeux relatifs au partage d'accès à l'espace santé sont considérables.

Avant de décider d'autoriser le partage, l'usager responsable d'un espace santé a intérêt à utiliser une grille d'aide à la décision afin de se donner les capacités de prendre en considération les enjeux et risques associés au partage.

3.2.4.2 La consultation

En vertu de l'article 23 de la *Loi concernant le cadre juridique des technologies de l'information*, lorsqu'une personne a accès à un document, celui-ci doit être consultable directement ou en faisant appel aux technologies de l'information.

Dans le contexte de l'ESP, le droit d'ouvrir un document à la consultation est exercé par le titulaire de l'ESP.

a) L'obligation de protéger les renseignements confidentiels

[51] Aarathi PRASAD, Jacob SORBER, Timoyhy STABLEIN, Denise L. ANTHONY and David KOTZ, « Understanding User Privacy Preferences for MHealth Data Sharing », dans MHealth Multidisciplinary Verticals, ch. 30, no. 30.2.3.

L'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* impose à la personne exerçant le contrôle à l'égard d'un document de prendre les mesures afin de protéger les renseignements confidentiels. Cela suppose de prendre les mesures de sécurité propres à en assurer la confidentialité. Au nombre des moyens qui peuvent être utilisés, il y a le contrôle d'accès effectué au moyen d'un procédé de visibilité réduite (par exemple, rendre des données invisibles à l'écran); d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement (par exemple, en exigeant que les personnes autorisées donnent un mot de passe avant d'accéder à l'information); ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder (par exemple, le système doit être configuré de manière à ce qu'il ne soit pas possible d'accéder de façon détournée à un document ou aux renseignements confidentiels).

Dans le contexte de l'ESP cela se traduit par l'obligation d'activer les configurations qui réservent à des catégories de personnes déterminées, la faculté d'accéder et de consulter certains documents. Si le titulaire de l'ESP néglige d'effectuer de telles configurations, il pourra se rendre responsable des conséquences qui pourraient en découler.

b) Les obligations à respecter lorsqu'un document technologique est confié à un tiers

Dans l'ESP, la situation en vertu de laquelle un usager autorise un tiers à exercer un contrôle sur des documents consignés dans son espace santé personnel revient à confier le document à ce tiers. Le législateur a prévu les principes à respecter lorsqu'un tiers détient des documents technologiques pour le compte d'un autre.

L'article 26 se lit comme suit :

> ***26.*** *Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.*
>
> *Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue dans la loi relativement à la conservation du document.*

Cette disposition vise aussi les situations où un document technologique, en l'occurrence ici, un ESP est confié à un prestataire de services (par exemple, l'archivage de documents hors site) pour qu'il en assure la garde. Il en est ainsi de TELUS en sa qualité de prestataire de services d'informatique distribuée, d'infonuagique[52] ou d'informatique en nuage (de l'anglais « Cloud computing ») comme solution informatique.

La personne qui confie le document à un prestataire de services pour en assurer la garde a l'obligation d'informer ce dernier de la protection que requiert le document et ce, lors de la remise du document. Il lui faut donner des informations adéquates sur les mesures de protection de la confidentialité que le document nécessite. Il faut pareillement indiquer quelles sont les personnes habilitées à en prendre connaissance.

---

[52] Terme retenu par l'Office québécois de la langue française. Disponible au : < http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp >.

De son côté, le prestataire de services doit faire en sorte que les moyens technologiques convenus d'un commun accord avec la personne qui lui a confié le document soient mis en place durant toute la période pendant laquelle il en la garde.

Ainsi, il est tenu, durant la période où il en a la garde, de voir à ce que les moyens technologiques soient mis en place pour :

- en assurer la sécurité,
- en préserver l'intégrité et,
- le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance.

Au surplus, le prestataire a l'obligation de respecter toute autre obligation prévue dans une loi relativement à la conservation d'un document.

Compte tenu de ces exigences, le contrat de prestation visé à l'article 26 doit être consigné dans un écrit et préciser les mesures relatives à la conservation sécuritaire des renseignements personnels. Le prestataire ne devrait pas conserver les documents à la fin de son mandat. Les prestataires sont en principe tenus aux mêmes obligations que les organismes détenteurs d'un document technologique. Il revient cependant à la personne qui confie le document d'indiquer les exigences auxquelles est soumis le document.

Dans plusieurs modèles d'infonuagique, le prestataire de services n'assume aucun rôle au regard de l'accès et des traitements des documents. C'est l'entité qui choisit d'y placer des documents qui demeure investie de toutes les prérogatives au regard de ces documents[53].

3.2.5 La transmission

Les documents technologiques se trouvant dans l'espace santé personnel peuvent être transmis à d'autres personnes, soit à l'intérieur du système (de la plate-forme) ou à une autre personne qui a un espace sur la même plate-forme ou une autre qui est compatible avec celle-ci.

La règle qui s'applique en matière de transmission repose sur l'exigence de la préservation de l'intégrité du document. L'article 30 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit à cet égard que le document technologique reçu aura la même valeur que le document transmis si les conditions suivantes sont respectées :

- le mode de transmission choisi doit permettre de préserver l'intégrité des deux documents;
- la documentation établissant la capacité d'un mode de transmission d'en préserver l'intégrité doit être disponible pour production en preuve, le cas échéant.

Par contre, le seul fait que le document ait été fragmenté, compressé ou remisé en cours de transmission pour un temps limité afin de la rendre plus efficace n'emporte pas la conclusion qu'il y a atteinte à l'intégrité du document. Il s'agit là d'une application des principes des articles 4, 5 et 10 de la loi qui établissent que la valeur juridique d'un document est fonction de son intégrité et qu'elle ne dépend pas de détails de forme.

---

[53] Sur ces aspects, voir : Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 125 et suiv.

Ainsi, si le document est transmis vers un autre espace de la plate-forme sécurisée, les mécanismes de certification et d'horodatage de même que les identifiants associés au document vont constituer un mode de transmission qui permet de préserver l'intégrité des deux documents (le document transmis et le document reçu).

Si le document est transmis en dehors de la plate-forme, il sera possible d'établir qu'au moment où il est sorti de la plateforme, le document a été transmis dans un système qui assurait la préservation de l'intégrité.

3.2.6 La signature

Lorsqu'un document doit être transmis et communiqué à une personne soignante via la plate-forme, celui-ci est horodaté et signé électroniquement lorsqu'il sort de l'espace personnel d'un patient ou d'un professionnel et est communiqué. Le document présente des caractéristiques qui assurent le lien entre la personne (l'utilisateur) et le document. Le document est doté également d'une marque constituant une signature. Ainsi, doté de ces caractéristiques, le document émanant de cet environnement peut être tenu pour intègre et de ce fait est pleinement admissible en preuve.

L'article 39 établit le principe de l'équivalence des signatures quel que soit leur support pourvu qu'elles répondent aux mêmes critères légaux, à savoir ceux qui sont prévus à l'article 2827 du *Code civil*.

> ***39.*** *Quel que soit le support du document, la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.*
>
> *La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu.*

L'article 2827 du *Code civil* prévoit que:

> ***2827****. La signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.*[54]

Cette définition générale du *Code civil* fait appel aux notions de « marque personnelle » et « d'usage courant » de cette marque comme manifestation du consentement. L'apposition de la marque personnelle d'une personne sur un document implique un lien durable entre la signature et le document.

La *Loi concernant le cadre juridique des technologies de l'information* vise à assurer l'établissement du lien qui permet de relier un document qui est sur un support faisant appel aux technologies de l'information à ceux qui communiquent par ce moyen. À cette fin, elle énonce les critères et les qualités requises des mécanismes utilisés afin d'établir un tel lien. L'article 38 de la loi précise les caractéristique que doivent posséder les procédés ou la combinaison de moyens auxquels il est fait recours. Autrement dit, pour déterminer si le mécanisme mis en place permet d'apposer des signatures à des documents, il faut se demander s'il rend possible l'association d'une marque

---

[54] L'article 77 de la *Loi concernant le cadre juridique des technologies de l'information* a remplacé dans l'article 2827 C.c.Q. le mot « sur » par le mot « à » (un acte).

personnelle à un document technologique. Lorsqu'une telle association existe, on est en présence d'une signature au sens de l'article 2827 du Code civil.

La signature est une marque pouvant servir à une multitude de fins. Par exemple, un artiste peintre peut apposer sa signature sur une toile. Mais l'article 2827 du *Code civil* retient la notion de signature en tant que marque utilisée afin de manifester un consentement. On vise ici le volet intentionnel de la signature, celui qui s'attache à l'état d'esprit de la personne qui pose la marque au document. Pour engendrer des effets juridiques, c'est-à-dire pour obliger le signataire, il faut qu'il y une intention du signataire de se lier par le geste déclenchant la signature.

Plusieurs particularités de l'espace santé personnel permettent d'assurer le caractère personnel d'une marque. La marque est utilisée à la suite d'un processus de vérification d'identité. Au moment de l'inscription d'un utilisateur et de la remise de son certificat, une vérification d'identité a été effectuée qui constitue la première étape du processus donnant lieu à la mise en service d'un certificat.

Dans la mesure où il permet de réaliser des documents technologiques présentant un lien entre une personne et un document, l'espace santé personnel doit nécessairement offrir une solution qui permet d'avoir des documents portant une signature tout à fait admissible en preuve et répondant aux conditions des lois qui exigent qu'un document soit signé.

En somme, lorsqu'on utilise les fonctions d'encryptage de manière à générer une marque associée à un document technologique et que cette marque est générée en vue de manifester un consentement, il y a signature électronique au sens de la loi. Le deuxième alinéa de l'article 39 ajoute des critères d'opposabilité à la signature d'un document technologique. Premièrement, l'intégrité du document doit être assurée, et deuxièmement le lien entre la signature et le document doit être maintenu. Les fonctions d'un tel espace doivent être conçues afin de procurer un tel résultat.

3.2.7 La fin de l'utilisation de l'espace santé personnel par le participant

Il y a des enjeux à considérer à l'égard de la fin de l'utilisation de l'espace santé personnel par le participant. Soit que l'utilisation cesse volontairement ou résulte de l'incapacité d'agir du participant. Dans toutes ces situations, il faut prévoir comment recevoir et traiter les demandes de révocation, de suspension ou de réactivation des certificats.

Selon notre compréhension, ces demandes s'effectuent en ligne sur la plate-forme via une fonction mise à la disposition des utilisateurs qui constatent que leur certificat a été compromis ou souhaitent interrompre leur activité dans l'espace santé personnel ou encore souhaitent y revenir.

3.2.7.1 La cessation volontaire

Le participant peut décider volontairement de mettre fin à ses relations avec l'espace santé personnel. Il s'agit alors de la résiliation du contrat avec le fournisseur du service.

Il sera opportun de préciser comment se fait la résiliation. Les conditions associées à la résiliation devraient prévoir les conditions d'archivage ou éventuellement de destruction des documents que l'usage a consigné ou autorisé dans son espace santé.

3.2.7.2 L'incapacité d'agir du participant

L'espace santé personnel peut être accédé par la personne à qui l'espace appartient ou par son mandataire autorisé[55].

En cas d'incapacité d'agir du participant, les lois prévoient de désigner un mandataire qui agira en son nom. Un tel mandataire devra forcément être enregistré à ce titre. Il pourrait s'agir d'un tuteur ou d'une personne disposant d'un mandat donné en cas d'inaptitude. Une fois enregistré, le mandataire doté d'un identifiant spécifique comprenant notamment un certificat d'attribut attestant de son statut de mandataire, pourra accéder à l'espace personnel.

En cas de décès du titulaire de l'espace de santé personnel, ce sont les représentants légaux qui peuvent obtenir la déséquestration des données. Il est prévisible que sera suivie une pratique semblable à celle des institutions financières offrant des espaces de coffre-fort, soit d'exiger la preuve du décès de même que la production de documents qui attestent du droit de la personne d'agir au nom de la succession de la personne décédée.

[55] Droit de la famille — 07578, 2007 QCCS 2276; Droit de la famille — 09667, 2009 QCCA 568.

4. Les responsabilités

Les enjeux et risques associés à un environnement comme l'espace santé personnel découlent aussi des responsabilités incombant aux acteurs impliqués dans le projet.

4.1 Du participant

Le participant dispose du plein contrôle sur les documents qu'il décide de mettre dans son espace santé personnel. Il est le seul à avoir la maîtrise, le contrôle de ce qui entre, sort et demeure dans son espace.

4.1.1 Tenir compte de la sensibilité des informations contenues dans son espace santé personnel

Il est donc particulièrement important que le participant soit informé et qu'il soit en mesure de prendre conscience des risques de partager avec des tiers des informations sur son dossier médical, son DSQ de même que d'autres informations sur son état de santé.

Étant donné le haut degré de sensibilité des informations concernées, il n'est pas excessif d'exiger que des mesures adaptées aux niveaux cognitifs des différents usagers soient mises en place afin de les informer adéquatement et de façon significative des enjeux et risques inhérents à un partage tel que celui que permet l'ESP.

Selon le contexte organisationnel dans lequel est déployé l'ESP, la responsabilité de procurer cette information adaptée à l'usager pourra revenir à la clinique, au professionnel de la santé concerné ou à d'autres types d'intervenants.

Le participant est doté de toutes les capacités afin de contrôler son espace. Il se trouve dans un environnement dans lequel il lui est permis d'intervenir pour ajouter et éventuellement retirer des documents.

La maîtrise par le participant concerne aussi bien la production d'information que les interactions qui prennent place à l'occasion de divers évènements. Selon le type d'activités auxquelles s'adonne le participant, diverses règles pourront trouver application. Il lui incombe donc de connaître et de gérer les divers types d'enjeux et risques inhérents aux activités qu'il mène dans son espace santé personnel.

4.1.2 Protéger ses identifiants

Les identifiants constituent le support des certificats et en pratique est une pièce essentielle pour accéder à la plate-forme. Ils sont en possession du participant et il a l'obligation de les protéger puisqu'ils qui lui permettent de s'identifier dans le système.

L'article 41 de la *Loi concernant le cadre juridique des technologies de l'information* impose à la personne qui les aura fait valoir, la responsabilité de conserver ces pièces importantes, qu'elles aient servi à établir sa propre identité ou celle d'une autre.

> ***41.*** *Quiconque fait valoir, pour preuve de son identité ou de celle d'une autre personne, un document technologique qui présente une caractéristique personnelle, une connaissance*

> *particulière ou qui indique que la personne devant être identifiée possède un objet qui lui est propre, est tenu de préserver l'intégrité du document qu'il présente.*

Les documents présentés au soutien d'une demande d'identification constituent les pièces justificatives sur lesquelles l'agent vérificateur s'appuie pour certifier l'identification. De tels documents doivent donc être conservés, et leur intégrité doit être préservée, notamment à des fins de vérification ou de renouvellement de l'identification.

L'article 41 impose aussi l'obligation de protéger le document contre l'interception s'il est conservé ou transmis sur un réseau de communication et pourrait être utilisé pour usurper l'identité de la personne identifiée. La confidentialité du document doit également être protégée en pareil cas et sa consultation journalisée. La journalisation fait référence à l'inscription des différentes consultations qui seront faites du document dans un fichier nommé journal ou « log », et la conservation de ce fichier pour référence future. Or, l'espace santé personnel, avec ses fonctions de sécurité élevées procure forcément une telle journalisation.

Les contrats régissant les relations entre un émetteur et le détenteur d'un identifiant prévoient généralement l'obligation de signaler la perte de l'identifiant car cela entraine la compromission possible du certificat.

4.1.3 Activer les configurations d'accès à son espace santé personnel

Dans le contexte de l'ESP, le droit d'ouvrir un document à la consultation est exercé par le titulaire de l'ESP. La loi impose à la personne exerçant le contrôle à l'égard d'un document de prendre entre autres des mesures de sécurité afin de protéger les renseignements confidentiels comme un contrôle d'accès ou un procédé qui empêche une personne non autorisée de prendre connaissance des renseignements ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder (art. 25).

Dans le contexte de l'ESP, cela se traduit par l'obligation d'activer les configurations qui réservent à des catégories de personnes déterminées, la faculté d'accéder et de consulter certains documents. Si le titulaire de l'ESP néglige d'effectuer de telles configurations, il pourra se rendre responsable des conséquences qui pourraient en découler.

4.1.4 Tenir à jour ses informations

L'usager a le devoir de tenir à jour les informations qui le concernent. L'article 59 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit une obligation de tenue à jour des renseignements qui ont été fournis en vue de l'obtention d'un certificat et ce dans les meilleurs délais.

4.2 De la clinique et professionnels de la santé

Quel est le statut et la position de la clinique et des professionnels de la santé impliqués à l'égard des informations versées dans l'espace santé personnel ?

Pour l'heure, une mention dans les interfaces du système avertit que les professionnels de la santé concernés ne s'engagent pas à prendre connaissance des informations transmises par les patients ou d'autres intervenants.

Comme le souligne le *Guide sur les dossiers électroniques* de l'Association canadienne de protection médicale, l'information contenue dans un dossier de santé électronique géré par un patient peut

présenter une fiabilité déficiente et cela ne relève pas le médecin de ses obligations de tenir ses dossiers ni de réaliser l'évaluation individualisée des patients. Il convient d'être prudent lorsqu'on se fie exclusivement à ces renseignements.[56]

Les obligations du médecin relatives au traitement de l'information en vertu des lois sur les services de santé et services sociaux, code de déontologie, qui régissent la pratique médicale et les autres pratiques professionnelles concernées peuvent prendre une dimension différente lorsqu'il y a usage d'un portail d'échange tel que l'ESP.

Le contrat médical suppose quatre obligations incombant au médecin: l'obligation de renseigner, l'obligation de respecter le secret médical, l'obligation de soigner et l'obligation de suivre le patient. L'obligation de renseigner, celle du respect du secret de même que l'obligation de suivre sont particulièrement interpelées lorsqu'on examine les enjeux d'un environnement de partage d'information sur la santé d'un patient.

4.2.1. Les obligations de suivre et d'informer

L'obligation de suivre découle des devoirs du médecin tel que reconnu par les règles de la responsabilité civile et des décisions qui en découlent et de la loi. L'article 5 de la *Loi sur les services de santé et les services sociaux* prévoit :

> *5.Toute personne a le droit de recevoir des services de santé et des services sociaux adéquats sur les plans à la fois scientifique, humain et social,* ***avec continuité*** *et de façon personnalisée et sécuritaire.*

Le *Code de déontologie des médecins* précise, à son article 32 à la section «Prise en charge et suivi» :

> *32.Le médecin qui a examiné, investigué ou traité un patient est responsable d'assurer le suivi médical requis par l'état du patient, à la suite de son intervention, à moins de s'être assuré qu'un autre médecin, un autre professionnel ou une autre personne habilitée puisse le faire à sa place.*
>
> *Le médecin qui signe une ordonnance collective ou visant l'ajustement d'un médicament ou de la thérapie médicamenteuse doit s'assurer qu'elle comporte des mesures visant la prise en charge ou le suivi médical, lorsque requis.*

Ce qui fonde l'obligation de suivre est l'impératif de continuité des soins. Dès qu'un médecin entreprend de prodiguer des soins à un patient et en devient le médecin traitant, il doit assumer avec compétence le suivi qui est approprié, compte tenu de tout problème signalé par le patient et ce jusqu'à ce qu'il ait donné un congé définitif au patient ou, s'il ne peut assurer lui-même le suivi, qu'il ait pris des mesures pour qu'un suivi de qualité soit assuré au patient.[57]

Non seulement le médecin a le devoir de ne pas abandonner le patient, mais le médecin doit demeurer disponible. L'article 37 du *Code de déontologie des médecins* précise à cet égard que :

---

[56] ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE, *Guide sur les dossiers électroniques*, 2014, p. 34.< https://www.cmpa-acpm.ca/fr/web/guest/-/electronic-records-handbook >

[57] Jean-Pierre MÉNARD, «L'obligation de suivre du chirurgien», *Développements récents en droit médico-légal et responsabilité des chirurgiens (2011*), Service de la formation continue du Barreau du Québec, 2011, p. 4.

> *37. Le médecin doit être diligent et faire preuve d'une disponibilité raisonnable envers son patient et les patients pour lesquels il assume une responsabilité de garde.*

Cette obligation est modulée en fonction du type de pratique et est plus exigeante en contexte hospitalier. Pour le médecin en bureau privé, on ne peut s'attendre à une disponibilité en tout temps et la clientèle est au courant «*mais il est important d'informer les patients de ce qu'ils doivent faire et de l'endroit auquel ils peuvent s'adresser pour des soins urgents*».[58]

L'utilisation de l'ESP par un patient peut lui fournir des informations en temps opportun sur son état de santé et l'encourager à participer activement à ses propres soins mais peut aussi engendrer de grandes attentes qu'il est nécessaire de clarifier avant son utilisation.

La façon dont l'ESP du patient sera utilisé pour communiquer en ligne doit être précisée avant son utilisation et la discussion, consignée au dossier[59]. Il faut informer le patient de ne pas utiliser son ESP lorsqu'il a un problème de santé urgent ou qui exige une réponse rapide et l'orienter vers une ressource d'urgence. Par exemple, pour gérer les risques reliés à l'utilisation d'un moyen de communication électronique, l'Association canadienne de protection médicale (ACPM) propose la condition d'utilisation suivante :

> *Bien que le médecin s'efforce de lire et de répondre promptement aux communications électroniques, il ne peut pas garantir qu'il les lira ou y répondra dans un délai précis. Par conséquent, les Services ne doivent pas être utilisés dans les cas d'urgence médicale ou d'autres situations devant être traitées rapidement.*
>
> *Si une communication électronique nécessite ou demande la réponse du médecin et qu'aucune réponse n'est reçue dans un délai raisonnable, il incombe au patient de faire un suivi afin de déterminer si le destinataire visé a bien reçu la communication , et à quel moment celui-ci y répondra.*[60]

S'agissant de l'utilisation d'un portail, l'ACPM mentionne :

> *Le médecin doit expliquer quels renseignements seront accessibles et partagés sur le portail. En outre, le médecin doit comprendre et préciser que certains renseignements ne peuvent être partagés en ligne, et qu'une consultation en personne peut s'avérer nécessaire pour éviter qu'un patient n'interprète mal les résultats ou pour discuter de la nécessité de soins de suivi.*[61]

Par exemple, dans le *Formulaire type de consentement à l'utilisation d'un moyen de communication électronique entre un médecin et un patient* de l'ACPM, on informe le participant des risques d'avoir recours aux communications électroniques pour discuter de renseignements de santé de nature délicate. Les conditions d'utilisation prévoient que les services de communication électronique patient-médecin ne doivent pas être utilisés pour communiquer des renseignements tels les maladies

---

58 Suzanne PHILIPS-NOOTENS, Pauline LESAGE-JARJOURA et Robert P.KOURI, *Éléments de responsabilité civile médicale – Le droit dans le quotidien de la médecine*, 3e édition, Éditions Yvon Blais, 2007, no. 359.

59 Voir ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE, *Les communications électroniques et les renseignements personnels*, octobre 2013.

60 ACPM, *Formulaire type de consentement à l'utilisation d'un moyen de communication électronique entre un médecin et un patient*. Ce formulaire est un outil proposé par l'ACPM dans sa Boîte d'outils pour gérer les risques médico-légaux en cabinet.

61 ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE, *Les communications électroniques et les renseignements personnels*, octobre 2013.

transmises sexuellement, le sida/VIH, la santé mentale, les déficiences développementales, l'abus d'alcool ou d'autres substances. Ces sujets ne peuvent être traités par communication électronique entre un patient et son médecin. Donc encore moins lorsqu'un patient partage son dossier avec une autre personne, membre de sa famille ou autre.

C'est donc dire que les formulaires de consentement ainsi que les conditions d'utilisation doivent être explicites quant aux limites de la communication patient-médecin via un outil tel l'ESP.

D'ailleurs, l'ESP est une forme de télémédecine[62] puisqu'il est possible de l'assimiler à de la télésurveillance, soit «le monitorage à distance par un médecin de données cliniques, radiologiques ou biologiques d'un patient transmises par TIC, qu'elles soient recueillies par le patient lui-même, un médecin ou un autre professionnel de la santé à des fins de diagnostic ou de traitement». Et, selon le Collège des médecins, dans tous les cas de télémédecine, l'information nécessaire à un consentement libre et éclairé du patient doit inclure ce qui concerne les moyens de télécommunication utilisée, dont :

- Les limites de l'exercice médical compte tenu des moyens de communication utilisés;
- Les bris possibles de confidentialité liés aux moyens de communication utilisés;
- La conservation de renseignements sur support électronique[63]

Ces aspects du consentement qui sont particuliers à la télémédecine doivent être documentés au dossier du patient (qui peut prendre la forme d'une «convention de communication») indiquant les canaux de communication qui seront utilisés et les personnes qui recevront ces communications[64].

Dans le contexte d'une utilisation de l'ESP, il paraît que c'est la clinique ou le professionnel de la santé qui est engagé dans une relation de soins qui est le mieux en mesure d'informer le patient des avantages mais aussi des enjeux et risques inhérents à l'ESP. En particulier, il faut que le patient soit clairement et complètement informé des enjeux et risques inhérents au partage des informations de son ESP avec les tiers qu'il autorise.

4.2.2 L'obligation de préserver le secret médical lors de l'utilisation de technologies de l'information

Le respect du secret professionnel fait partie intégrante du contrat de soins entre le médecin et le patient. Cette obligation fut d'abord déontologique avant d'être légale mais « ses assises dans le droit positif sont incontestables»[65].

Le Code de déontologie des médecins a été modifié en janvier 2015, en particulier les dispositions sur le secret médical, afin de tenir compte de l'utilisation grandissante par les médecins des nouvelles technologies de l'information et des réseaux sociaux.

---

62 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 9.

63 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 15.

64 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 15.

65 Article 9 de la *Charte des droits et libertés de la personne* ; Article 20 du *Code de déontologie des médecins, (RLRQ, c. M-9, r.17), règlement édicté en vertu de la Loi médicale et du Code des professions* et entré en vigueur le 7 janvier 2015.

Le médecin doit garder confidentiel ce qui est venu à sa connaissance dans l'exercice de sa profession (art. 20 (1) Code de déontologie). Il doit aussi prendre les moyens raisonnables à l'égard des personnes qui collaborent avec lui, par exemple l'équipe de soins, pour que soit préservé le secret professionnel (art. 20 (3)).

L'obligation au secret professionnel se traduit par des devoirs spécifiques lorsque le médecin utilise les technologies de l'information pour interagir avec le patient :

> *20. Le médecin, aux fins de préserver le* ***secret professionnel****:*
>
> *[…]*
>
> *8° doit prendre les moyens raisonnables pour que soit préservé le secret professionnel lorsqu'il utilise ou que des personnes qui collaborent avec lui utilisent les technologies de l'information;*

La *Loi concernant le cadre juridique des informations* prévoit aussi que la confidentialité des renseignements doit être protégée par un moyen approprié au mode de transmission, y compris sur les réseaux de communication (art. 34)

Il appartient donc au médecin d'évaluer si les technologies de l'information utilisées pour communiquer avec son patient permettent de préserver le secret professionnel. Il doit agir avec prudence et diligence en s'informant et en mesurant les risques de l'utilisation d'une technologie de l'information par rapport au degré de sensibilité de l'information à transmettre.

Tel que mentionné, le médecin doit convenir avec son patient des modes de communication mais aussi des moyens de protection qu'il utilisera en fonction de l'information en cause et cette convention doit être documentée. Et même avec une telle convention, le médecin demeure responsable d'assurer la protection du secret professionnel et la confidentialité des informations qu'il transmet et il se pourrait qu'il doive adapter le mode de communication avec son patient aux circonstances du moment selon la nature des informations[66].

S'il utilise l'ESP pour partager de l'information avec son patient, le médecin a le devoir d'informer le patient des limites de cette technologie non seulement en terme de communication (délai de réponse…) mais également relativement à la confidentialité des échanges.

4.2.3 L'obligation de préserver le secret médical lors de transmission d'information contenue au dossier médical

Un des aspects particuliers du secret professionnel concerne la confidentialité du dossier médical. Le médecin a l'obligation de protéger les renseignements confidentiels contenus au dossier médical du patient et en restreindre l'accès aux seules personnes autorisées[67]. Le patient est maître des informations confidentielles contenues dans son dossier médical et le médecin en est le gardien.

Lorsqu'il y a transmission d'informations contenues dans les dossiers médicaux par des moyens technologiques, par exemple, lorsque des données du dossier médical sont transférées par le

---

66 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 18.

67 Art. 11 al. 1, *Règlement sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin*, chapitre M-9, r. 20.3.

médecin et l'équipe de soins vers l'ESP du patient, «le médecin doit utiliser des méthodes, des appareils ou des systèmes protégeant la confidentialité de ces informations»[68] .

Ainsi, la transmission d'une ordonnance médicale sur support électronique implique un niveau de confiance supérieure qui requiert l'utilisation d'une signature numérique afin de s'assurer qu'aucune falsification ne soit possible alors que l'identification à l'aide d'un nom d'usager et d'un mot de passe est un procédé de signature suffisant pour les renseignements médicaux versés au DMÉ ou au DSQ[69].

La transmission d'informations issues du dossier médical d'un patient vers l'ESP est une opération assujettie à ce devoir du médecin de préserver le secret médical.

Étant donné les caractéristiques intrinsèques de l'ESP, en particulier, les facultés qu'il procure de partager avec des tiers des informations issues du dossier médical, il est nécessaire que le médecin ou autre professionnel de la santé concerné informe explicitement le patient des conséquences d'un tel transfert. En somme, le transfert dans l'ESP a pour conséquence de remettre au patient la maîtrise de l'information provenant de son dossier médical.

4.2.4 L'obligation de consigner et de documenter les données de monitorage dans le dossier médical

Toutes les informations et les conseils donnés au médecin au moyen des technologies de l'information, qu'ils proviennent du patient ou d'un membre de l'équipe de soins doivent être consignés au dossier du patient. Cela inclut tous les courriels et textos envoyés ou reçus.

Lorsque des paramètres biologiques et des données de monitorage sont fournis au médecin par son patient (glycémie, prise de tension artérielle) ou par des tiers, le médecin doit documenter dans le dossier du patient la technologie utilisée et les conditions définies avec le patient afin de s'assurer de la validité de ces paramètres[70].

Le Guide de l'ACPM met d'ailleurs en garde les médecins sur la fiabilité des données contenues dans les dossiers de santé électronique créés par les patients :

> *Puisque l'information contenue dans un dossier de santé électronique géré par un patient peut manquer de fiabilité, les médecins doivent faire preuve de prudence s'ils se fient exclusivement à ces renseignements. Dans certaines circonstances, il peut être aussi prudent de vérifier l'exactitude et l'exhaustivité de l'information. Les dossiers de santé créés par les patients ne libèrent pas le médecin de ses obligations de tenir ses propres dossiers ni de réaliser l'évaluation individualisée des patients, notamment en posant des questions sur leurs antécédents médicaux. Lorsqu'un patient demande au médecin de verser de l'information dans un dossier de santé en ligne, le médecin devrait discuter de cette demande avec le patient, et passer minutieusement en revue les questions de consentement et de sécurité.*[71]

---

68 Art. 11 al. 2, *Règlement sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin*, chapitre M-9, r. 20.3.

69 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 32.

70 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 33.

71 ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE, *Guide sur les dossiers électroniques*, 2014, p. 34.

4.2.5 L'obligation d'assurer l'intégrité des données médicales

Tel que précisé, les données de l'ESP sont des documents technologiques. La communication ou le partage des données médicales dans l'ESP doit se faire dans un environnement où l'intégrité des données est assurée. L'article 6 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit les conditions de l'intégrité d'un document technologique :

> *6. L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.*
>
> *L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.*
>
> *Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.*

L'ESP doit présenter des fonctionnalités permettant l'identification de tous les utilisateurs et la journalisation des accès au document et garantir l'inaltérabilité des transactions («toute transaction doit être enregistrée, ne peut être modifiée lorsque signée et les modifications subséquentes doivent être «retraçables»)[72]. La communication ou le partage des données doit permettre d'identifier sans équivoque l'auteur de l'envoi et le récepteur de l'envoi tout en assurant la confidentialité de la communication.

4.2.6 L'obligation de préserver le secret professionnel de chaque membre du couple ou de la famille

Lors de l'inscription à l'espace santé TELUS, l'utilisateur peut ajouter plus d'un dossier à son compte. Pour ajouter une nouvelle personne à son compte, que ce soit les membres de sa famille, conjoint ou tout autre personne, l'utilisateur doit avoir une invitation à partager en provenance de la clinique. Une fois l'invitation en main, l'utilisateur peut compléter l'inscription et ajouter le dossier à son compte. Il peut alors basculer d'un profil à l'autre et gérer la santé de plusieurs membres de sa famille.

Par exemple, pour *l'inscription d'un enfant par le parent*, le parent reçoit de la clinique le courriel qui contient l'invitation pour la connexion au dossier de l'enfant aux données en provenance du DMÉ et l'accès à l'application du ESP. À partir de son propre compte, le parent autorise ensuite les deux applications (soit le DMÉ et l'ESP) à accéder au dossier de l'enfant. Une fois l'autorisation en place, le DMÉ est autorisé à téléverser des données au dossier de l'enfant en tout temps. Le parent peut donc consulter les données transmises par l'équipe clinique au moyen du ESP. Et une fois qu'il est gestionnaire du compte de son enfant, il peut autoriser qui il veut à accéder aux données de l'espace personnel de son enfant. Ainsi, un parent peut permettre au professeur de son enfant d'accéder au dossier de l'enfant pour compléter des questionnaires.

Au Québec, la capacité d'une personne de consentir aux soins est fixée à 14 ans. En deça de cet âge, un parent, un tuteur ou le tribunal doit consentir au traitement proposé. Qu'advient-il lorsqu'un adolescent devient apte à gérer son propre dossier?

---

[72] Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 29.

Un médecin qui assure le suivi de plusieurs membres d'une même famille doit être extrêmement vigilant et respecter son obligation au secret professionnel envers chacun des membres du couple ou de la famille. Le Code de déontologie des médecins prévoit :

> *20. Le médecin, aux fins de préserver le* secret professionnel*:*
>
> *[…]*
>
> *7° doit, lorsqu'il exerce auprès d'un couple ou d'une famille, sauvegarder le droit au secret professionnel de chaque membre du couple ou de la famille;*

Il ne peut prétendre avoir un consentement tacite par souci d'efficacité et permettre la transmission d'informations confidentielles entre membres d'une même famille sans leur consentement. La durée de l'invitation à partager d'un dossier d'un enfant devrait donc être limitée, soit jusqu'à ses quatorze ans.

En cas de séparation des conjoints ou autres modifications des relations familiales, se posent forcément d'importants enjeux quant à la discontinuation des droits d'accès à l'espace santé par un ancien conjoint ou par une personne à laquelle le titulaire de l'ESP souhaite retirer les droits qu'elle s'était vue conférer sur son espace santé.

Si a priori, la responsabilité d'agir dans de telles situations incombe au patient titulaire de l'ESP, il est impossible d'exclure complètement la responsabilité du médecin en de pareilles circonstances dans lesquelles le partage avec un tiers est autorisé.

4.2.7 L'obligation de documenter toute communication faite à un tiers d'un renseignement protégé par le secret médical

L'article 20 du Code de déontologie des médecins prévoit :

> *20. Le médecin, aux fins de préserver le secret professionnel:*
>
> *[…]*
>
> *9° doit documenter dans le dossier du patient toute communication faite à un tiers, avec ou sans le consentement du patient, d'un renseignement protégé par le secret professionnel.*

L'ESP doit donc procurer de telles fonctions assurant la documentation de telles communications.

4.2.8 L'obligation de documenter le dossier du patient

Deux aspects sont concernés au regard de l'obligation de documenter le dossier du patient lorsqu'il y a utilisation de l'ESP. Les renseignements partagés dans l'ESP et qui sont relatifs à une consultation médicale ou un suivi médical doivent être versés au dossier médical du patient. Lorsqu'il y a usage d'un DME, il importe que le transfert des informations associées aux soins et au suivi soient transférés dans le DME.

Il est donc essentiel qu'il existe un protocole clairement établi quant au statut des informations transitant dans l'ESP. Si ces informations ne sont pas vues ou validées par une personne soignante, il faut clairement déterminer quel est leur statut.

Lorsque, en tant que document technologique, l'ESP est modifié durant la période pendant laquelle il doit être conservé, des conditions doivent être respectées afin d'en préserver la valeur juridique en dépit de la modification (art. 21 de la *loi concernant le cadre juridique des technologies de l'information*). Si ces conditions n'étaient pas observées, il pourrait être considéré que la modification de l'information constitue une altération du document, ce qui lui ferait perdre son intégrité, qui fonde sa valeur juridique. Afin de préserver la valeur juridique de l'ESP en dépit de la modification, la personne qui a l'autorité pour faire la modification doit noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui, ainsi que la raison de la modification.

La modification ainsi effectuée fait partie intégrante du document même si elle se trouve sur un document distinct, et généralement les métadonnées génèrent la documentation requise par de telles exigences[73].

4.2.9 L'obligation d'assurer l'intégrité et la confidentialité de l'ESP

Comme le souligne le Collège des médecins, le dossier médical est en mutation profonde avec la généralisation des technologies de l'information; le dossier est désormais «éclaté» :

> *les éléments le constituant pouvant se retrouver dans les archives d'un ou plusieurs établissements, dans une clinique privée, dans l'ordinateur d'un ou plusieurs médecins et dans divers appareils technologiques intelligents, tant sur des serveurs au Québec qu'hors du Québec, bref dans une multitude d'endroits tantôt physiques, tantôt virtuels.*[74]

Dans un tel environnement, ce qui peut être tenu comme étant constitutif du dossier médical est susceptible d'être réparti en divers répertoires et il est impossible d'exclure que les informations se trouvant dans l'ESP soient considérées comme faisant fonctionnellement partie du dossier médical d'une personne.

Des enjeux et risques paraissent inhérents à une pareille « virtualisation » du dossier médical qui ne peut plus être considéré comme une unité informationnelle située dans un seul lieu.

4.2.10 La compatibilité avec la clause de non-responsabillité

La clause de non responsabilité portée à l'attention des personnes faisant usage de l'ESP dans le cadre de l'expérimentation pourra poser problème si cela devait un jour se dérouler en dehors d'un contexte expérimental. Le Code de déontologie des médecins dispose en effet que:

> *11. Le médecin doit, dans l'exercice de sa profession, engager pleinement sa responsabilité civile. Il ne peut l'éluder ou tenter de l'éluder, ni requérir d'un patient ou d'une personne une renonciation à ses recours en cas de faute professionnelle de sa part.*

L'utilisation d'un ESP assorti d'une clause d'exclusion de responsabilité paraît difficilement envisageable, compte tenu de l'économie générale du droit relatif à la responsabilité des médecins de même qu'aux principes déontologiques applicables. Dès lors que l'usage d'un ESP est intégré dans le déroulement d'une relation de soins, il faudra, pour assurer une maîtrise effective des enjeux et

---

73 David HRICIK and Chase Edward SCOTT, "Metadata : The Ghosts Haunting e-Documents", (2009) 26 *The Computer & Internet Lawyer*, 23-34, p. 24.

74 Collège des médecins, *Le médecin, la télémédecine et les technologies de l'information et de la communication*, guide d'exercice, 02/2015, p. 28.

risques que cela comporte que les conditions du déroulement de la relation de soins soient l'objet d'ajustements ou de révisions conséquentes.

4.3 Du prestataire de service

L'ESP est rendu disponible par un prestataire de service qui est tenu à certaines obligations en vertu de la *Loi concernant le cadre juridique des technologies de l'information*.

La responsabilité du prestataire de services d'ESP est de procurer et de maintenir les espaces à la disposition des usagers et de garantir que les fonctions annoncées de l'espace santé personnel sont en bon état de fonctionnement. La plupart des responsabilités qui lui incombent à l'égard des participants sont précisées dans les contrats qui lient le prestataire à chacun des participants.

Toutefois, la *Loi concernant le cadre juridique des technologies de l'information* énonce les règles générales relatives à la responsabilité de ceux qui assurent des services ou des fonctions relatives à des opérations effectuées en rapport avec des documents technologiques.

4.3.1 Le prestataire de service doit protéger la sécurité, l'intégrité et la confidentialité des documents

En vertu de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire de service a une obligation générale de protéger la sécurité, l'intégrité et la confidentialité des documents placés par les utilisateurs dans les espaces santé personnels. Aux termes de l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* :

> ***26.*** *Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue dans la loi relativement à la conservation du document.*

Toutefois, en vertu de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire de l'ESP ne peut prendre de moyens pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions. Par contre, les lois encadrant le travail de ces autorités chargées de la sécurité publique et de la prévention du crime, limitent les gestes que ces derniers peuvent poser. Ainsi, l'accès par les forces de police à des informations à caractère médical est généralement assujetti à l'obligation d'obtenir un mandat de perquisition.

Ainsi, sous peine d'engager sa propre responsabilité, le prestataire de service d'ESP ne peut s'interposer lorsque les autorités publiques demandent, conformément à la loi, d'accéder à des documents se trouvant dans un espace santé personnel dont il est le prestataire.

4.3.2 Le prestataire de service n'est pas tenu de surveiller

À l'instar de la directive européenne[75], l'article 27 de la *Loi concernant le cadre juridique des technologies de l'information* exclut l'obligation de surveillance active pour les intermédiaires tel que le prestataire de service de l'ESP. L'article 27 se lit comme suit :

> ***27.*** *Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite.*
>
> *Toutefois, il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.*

L'article 27 précise les obligations incombant au prestataire de services agissant « à titre d'intermédiaire pour fournir des services sur un réseau de communication », ou y conserve ou y transporte des documents technologiques.

Le prestataire d'ESP est visé par cette disposition. Il agit en effet à titre d'hébergeur, d'archiveur et même de transporteur. De plus, il fournit des services sur un réseau de communication et il conserve ou transporte des documents technologiques.

L'article 27 écarte l'obligation de surveillance active pour ce type d'intermédiaire. Ils ne sont pas tenus de surveiller l'information ni de rechercher des circonstances qui pourraient indiquer que des documents permettent la réalisation d'activités illicites. Mais le prestataire de l'ESP ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, conformément à la loi, notamment en ce qui a trait à la confidentialité. Ils ne doit pas non plus prendre de moyens pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions. Ce sont les lois encadrant le travail de ces autorités chargées de la sécurité publique et de la prévention du crime qui limitent les gestes que ces derniers peuvent poser.

Mais l'exclusion de l'obligation de surveillance active connaît des limites. Apparemment, elle prend fin lorsqu'un contenu effectivement illicite a été porté à la connaissance de l'intermédiaire.

---

75 L'article 15 de la *Directive sur le commerce électronique* se lit comme suit : 1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. 2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

4.3.3 Le prestataire de service n'a ni le droit de surveiller ni d'accéder aux données

Non seulement le prestataire n'a pas d'obligation de surveiller, il n'a pas le droit de surveiller. Tant les règles générales sur le droit à la vie privée que les impératifs de secret inhérents à la relation de soins de santé s'opposent à ce qu'un tiers qui n'est pas impliqué dans la relation de soins puisse prendre connaissance des informations qui sont consignées dans les environnements qui permettent le fonctionnement de l'espace santé personnel.

L'article 35 du Code civil affirme le droit à la vie privée et l'article 36 identifie certaines situations qui peuvent constituer des atteintes à la vie privée. Ainsi, l'article 36 dispose que :

> *Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:*
>
> *1° Pénétrer chez elle ou y prendre quoi que ce soit;*
>
> *2° Intercepter ou utiliser volontairement une communication privée;*
>
> *[...]*
>
> *6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.*

En somme, à moins qu'il existe des circonstances justifiant de mettre un usager sous surveillance, le prestataire de l'ESP ne peut surveiller les utilisateurs ou les autres participants de l'espace santé personnel.

De la même façon, en dehors de consentements explicites, il n'a pas le loisir de permettre à d'autres personnes que celles autorisées par un titulaire d'un ESP ou les personnes autorisées par la loi, d'accéder aux documents consignés dans les banques de données constituant l'ESP.

Ce sont ces règles de base qui régissent a priori le droit d'un prestataire de réaliser des traitements analytiques sur les données agglomérées qui sont consignées dans les serveurs de l'ESP. L'Association canadienne de protection médicale rappelle que « les patients et les professionnels de la santé doivent avoir l'assurance que les renseignements personnels sont protégés pour apporter leur appui à l'analyse des mégadonnées. »[76]

Par défaut, souligne l'Association canadienne de protection médicale, les traitements de mégadonnées devraient viser des informations anonymisées. Il est en effet essentiel que les usages des données ne portent que sur des répertoires présentant des garanties sérieuses à l'effet qu'il n'y aura pas de possibilité d'accès à des informations portant sur une personne identifiable sans consentement non équivoque de celle-ci.

4.3.4 Les situations où la responsabilité du prestataire de service pourra être engagée

L'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* clarifie, pour le droit québécois, les principes qui doivent trouver application dans un ensemble de situations dans

---

[76] ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE, *L'impact des mégadonnées sur les soins de santé et l'exercice de la médecine*, août 2014, p. 3, < https://www.cmpa-acpm.ca/documents/10179/301372750/com_14_big_data_design-f.pdf >

lesquelles le prestataire d'un service d'ESP n'exerce pas de contrôle à l'égard des informations fautives. Il se lit comme suit :

> ***22.*** *Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci [...].*

Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

Les deux premiers alinéas de l'article 22 visent l'intermédiaire offrant des services de conservation de documents technologiques sur un réseau de communication. C'est précisément le cas de figure représenté par l'espace santé personnel.

L'espace santé personnel procure en effet des fonctionnalités assurant la disponibilité de service de conservation de documents sur un réseau. Concrètement, il héberge les fichiers et autres répertoires d'information et de documents dans des serveurs sur lesquels il exerce un contrôle.

S'il est indéniable que l'hébergeur est techniquement en mesure d'accéder et de prendre connaissance de la teneur des documents hébergés sur ses installations techniques, il est également vrai qu'il se trouve dans une situation qui l'empêche pratiquement et légalement de prendre connaissance du contenu des documents et d'apprécier leur sens. La fonction éditoriale lui échappe : il n'a pas de droit de regard sur la teneur des documents hébergés.

La limitation de responsabilité profitant à l'hébergeur connaît toutefois des limites. Elle ne joue pas s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

Cette obligation de cesser promptement de fournir ses services aux personnes qu'il sait être engagées dans une activité illicite s'impose au prestataire lorsqu'est établie la connaissance du caractère illicite. La condition préalable à la responsabilité d'un prestataire intermédiaire est la connaissance du caractère fautif des documents situés dans un espace d'un utilisateur.

Dès qu'il acquiert la connaissance du fait que des personnes sont engagées dans une activité illicite, le prestataire de services a l'obligation de cesser promptement de fournir ses services.

4.4 Des fournisseurs d'applications logicielles

L'utilisation par un usager d'applications logicielles branchées à l'espace TELUS pour collecter et stocker des données dans son espace personnel pourrait soulève certains enjeux. Mais selon les informations disponibles, il n'est pas actuellement possible d'identifier exhaustivement ces enjeux. Il importe d'évaluer les droits et obligations de chacun à l'égard des informations collectées à partir de l'outil médical connecté à un ESP. Ces risques sont habituellement divulgués au niveau de l'outil médical connecté mais il subsiste la question de l'effet cumulatif du raccordement de l'ESP à un ensemble d'outils médicaux connectés. La question du traitement des informations recueillies à partir des outils médicaux et conservés par les serveurs associés à de tels outils se pose aussi. Des risques

significatifs de circulation d'information et de perte de confidentialité doivent ici être pris en considération.

Conclusion

Dans ce rapport, nous avons passé en revue les principaux risques et enjeux associés au projet pilote d'espace santé TELUS.

La revue des enjeux et risques a permis de situer les caractéristiques de l'application d'espace santé personnel TELUS. Cette application est dotée de caractéristiques assurant l'intégrité des documents technologiques qui y sont consignés de même que les mécanismes d'établissement des liens d'authenticité entre les personnes, les entreprises et un document.

L'ESP est un lieu de synchronisation entre le dossier médical électronique, le Dossier santé du Québec et les rapports informationnels inhérents à la relation de soins. Il habilite les différents acteurs de la relation de soins à agir de concert. Toutefois, cette capacité d'agir de concert vient avec les enjeux et risques découlant du partage d'information dans les cercles familiaux ou domestiques, dans l'espace clinique de même que dans les environnements analytiques qui pourraient avoir accès aux données transitant dans l'espace santé.

Emblématique de la tendance vers le basculement de la relation de soins dans l'espace des réseaux, l'ESP interconnecte les participants selon des modalités passablement différentes de celles qui caractérisent la relation classique de soins dispensés dans le cadre d'épisodes situés dans le temps et dans l'espace.

Les enjeux et risques que nous avons identifiés dans le présent rapport concernent les conditions d'accès et de partage des informations de santé consignées dans l'ESP.

L'analyse des enjeux et risques juridiques révèle la nécessité de porter attention aux conditions dans lesquelles le partage d'information peut être autorisé par les différents participants. Les variations qui surviennent forcément dans le statut des personnes impliquées dans le partage nécessitent un encadrement qui identifie mieux les enjeux de même que les précautions à envisager.

Les droits des entités intermédiaires à des fins analytiques présentent aussi de potentiels risques qu'il est nécessaire d'envisager afin de mieux délimiter l'ampleur et la portée de la faculté de traiter les données agglomérées et anonymisées transitant dans l'ESP.

Enfin, les échanges que permet l'ESP avec le DME et le DSQ engendrent des enjeux et risques au plan du cadre juridique régissant ces deux grands répertoires de données de santé.

En tant que lieu de synchronisation de l'information et de communication entre le patient, ses proches et les professionnels de la santé, l'ESP présente des enjeux et risques qui doivent être connus et pris en considération par tous.

De même l'organisation des soins doit refléter les possibilités de circulation résultant de l'usage de l'ESP.

Il est donc nécessaire d'informer adéquatement et complètement les patients et leurs proches sur les capacités d'agglomération d'information que procure l'usage de l'ESP.

En particulier, ceux qui autorisent l'accès à leurs informations de santé à d'autres personnes devraient être particulièrement bien au fait de ce que cela implique.

Par exemple, le versement d'information relative à la santé d'un proche dans un ESP peut engendrer des conséquences pour les participants à une telle mise en commun.

Lorsque le statut d'un participant à un ESP change, lorsque surviennent des modifications dans les relations entre les personnes, au sein du cercle familial ou quasi-familial, des mesures doivent être prévues afin de rompre les liens informationnels de rattachement avec les ESP des personnes concernées.

En particulier, lorsqu'un patient mineur atteint l'âge de 14 ou de 18 ans, il doit y avoir un mécanisme assurant la purge d'informations dans l'ESP du titulaire de l'autorité parentale à moins d'un consentement explicite au maintien d'une telle communauté d'accès au sein de l'ESP.

Il y a un défi véritable à assurer l'effectivité des retraits de consentement aux partages d'information au sein de l'ESP.

Le cas échéant, l'utilisation secondaire des données par les tiers devrait aussi être clairement connue et expliquée à tous les participants.

Récapitulatif des enjeux et risques de l'espace santé TELUS

Au terme de cette analyse des enjeux et risques des systèmes de partage d'informations dans le cadre de la relation entre le patient et le médecin telle qu'observé dans le contexte de l'espace santé TELUS, nous retenons les constats qui suivent.

L'ESP est un espace de partage et d'échange d'information.

La circulation accrue des informations de santé, par nature sensible, requiert des précautions.

À cet égard, l'identification, l'horodatage, la protection de l'intégrité physique des documents consignés dans l'espace santé doivent être conséquents avec la sensibilité inhérente des renseignements de santé.

Les potentialités d'accumulation et de couplage des informations sont plus considérables dans de tels réseaux que dans les échanges prenant place dans le cadre classique de la relation de soins.

Des risques d'ampleur différente peuvent dépendre des lieux où sont stockées les données : est-ce qu'elles sont conservés dans l'appareil médical porté par le patient ou dans l'infonuage du prestataire de services? Si, elles sont entreposées dans l'infonuage, il importe d'évaluer la durée et les conditions de cet entreposage, notamment au regard de l'application possible de lois nationales différentes de celles qui s'appliquent sur notre territoire.

Cela appelle des mécanismes qui assureront la protection des informations en tenant compte des avantages de la circulation des informations tout en minimisant les inconvénients.

Dans le contexte de l'espace santé, l'enjeu n'est plus tellement de savoir si une information peut ou non être en possession d'une autre personne que celle qui est directement concernée mais plutôt si cette dernière a le droit d'en faire usage pour prendre une décision dans une situation spécifique.

De l'épisode de soins au flot continu d'information

La relation de soins peut se trouver métamorphosée. La consultation médicale opère actuellement selon un modèle supposant le partage d'information entre le patient et le professionnel de la santé dans le cadre d'une rencontre située dans le temps et dans l'espace. Avec l'espace santé, on est en présence d'un modèle de flot continu d'information

D'une relation habituellement caractérisée par des épisodes de soins au cours desquelles le soignant et le soigné partagent des informations, le recours à l'ESP suppose un flux continu d'information. Il peut en découler des malentendus quant aux capacités ou possibilités pour le médecin de prendre effectivement connaissance des informations au ryhtme où elles sont transmises.

Les modes de pratique fondés sur des épisodes de rencontres fixés dans le temps ne sont pas nécessairement compatibles avec un partage d'information se déroulant en continu.

Les principaux enjeux et risques

Les enjeux et risques associés aux fonctions de partage se révèlent lorsqu'on examine les principales phases du *cycle de partage de l'information*.

- Le partage dans l'ESP est susceptible de priver d'effet les interdictions de communiquer des informations consignées dans le DSQ d'un patient. C'est un risque inhérent qui doit être connu et assumé par celui qui choisit d'utiliser un ESP.

- Le partage est initié par l'usager qui a le loisir d'attribuer des permissions d'accès. Ces permissions sont-elles graduables, en fonction des différents types de documents ?

- La décision d'autoriser le partage

  C'est à la personne concernée par les informations de santé qu'il revient a priori d'autoriser le partage. C'est une importante prérogative qui permet de donner à d'autres personnes l'accès aux informations de santé qui sont consignées dans son espace personnel.

  Dans certaines situations, c'est à une autre personne que revient la faculté d'autoriser un partage. Il s'agit typiquement de personnes de l'entourage du patient qui exerce l'autorité parentale ou qui agit en vertu d'un mandat de protection.

  Les titulaires de l'autorité parentale peuvent agir au nom des personnes mineures sous leur protection. À l'égard de ces usagers, se pose la question du départage des droits et responsabilités respectifs des titulaires de l'autorité parentale et des mineurs concernés lorsque la personne mineure atteint l'âge de quatorze ans puis l'âge de dix-huit ans.

  Certains agissent à titre de mandataires pour une personne inapte ou qui n'a pas été déclarée inapte bien qu'elle ne soit pas en mesure de prendre des décisions relatives à l'ESP.

  Un autre enjeu se rattache à l'ampleur des partage possibles.

  Les personnes qui ont l'autorisation de permettre le partage des informations consignées dans l'espace santé comme celles exerçant l'autorité parentale ou détentrices de mandats de protection ou en cas d'inaptitude peuvent, dans le contexte de l'ESP :

  - Accéder aux informations consignées dans l'espace santé

    Se pose la question de la mesure dans laquelle il est possible de baliser le partage de renseignements.

    Quels ajouts possibles aux renseignements? De quelle façon ces informations sont-elles validées?

    Quelles sont les informations qu'une personne autorisée à partager est en droit d'ajouter, de modifier ou de retrancher ?

    Quelles modifications possibles?

    Quelles suppressions ?

    La personne responsable du partage a la faculté de l'autoriser ou d'y mettre fin.

    À priori, la personne qui est titulaire de l'espace santé est celle qui autorise. Elle est donc responsable de l'accès aux documents consignés. Mais il importe de se demander si, dans le cadre d'un ESP cette responsabilité devrait ou non être partagée avec d'autres, avec la clinique ou le professionnel traitant.

    Dès lors que le partage peut être étendu sans limites, il pourrait s'avérer difficile d'attribuer une information se trouvant dans un ESP.

- L'information préalable aux patients

Il s'agit ici d'information relative à l'état de santé d'une personne. Il faut que le système de l'ESP soit organisé de façon à garantir que les patients soient effectivement et adéquatement informés des enjeux et risques spécifiques au partage.

La mesure dans laquelle les patients en position d'autoriser le partage d'informations sont informés des possibilités et des modes de fonctionnement du partage constitue un enjeu et une source importante de risque.

- Le contrôle de l'usager

  L'économie générale des règles en matière de protection des renseignements personnels milite en faveur de la reconnaissance effective d'un haut niveau de maîtrise au profit des usagers concernés par les informations.

  Les participants valorisent la capacité de contrôler et de décider quelle information partager, avec qui et dans quelles circonstances et apprécient la flexibilité des outils permettant de contrôler le partage. Le contrôle de l'information est ainsi un enjeu identifié par les usagers.

- Les conditions générales des accès à un espace santé

  L'ESP prévoit la gradation des droits d'accès : en fonction des enjeux associés aux différents niveaux de permissions : Lecture seulement, Modifications possibles, Pouvoirs complets

Avant de décider d'autoriser le partage, l'usager responsable d'un espace santé a intérêt à utiliser une grille d'aide à la décision afin de se donner les capacités de prendre en considération les enjeux et risques associés au partage et les différents niveaux possibles de permissions qu'il a le loisir d'accorder.

Le *partage entre le patient et des membres de sa famille ou des tiers* présente des enjeux lorsque surviennent des modifications dans les relations familiales ou autres.

Alors, il faut prévoir de quelle façon seront déterminées les conditions de la discontinuation des droits d'accès à l'espace santé par exemple, par un ancien conjoint ou par une personne à laquelle le titulaire de l'ESP souhaite retirer les droits qu'elle s'était vue conférer sur son espace santé

Dans le cas d'un parent invitant un tiers à partager le dossier de son enfant, certaines questions se posent : qu'arrive-t'il lorsqu'un adolescent devient, généralement lorsqu'il atteint l'âge de quatorze ans, apte à gérer son propre dossier?

Des interrogations similaires se posent à l'égard de tiers, par exemple, un entraîneur dans le cadre d'un programme de conditionnement physique ou un professionnel de la santé qui cesse de soigner le titulaire de l'ESP.

Il importe de prévoir un ensemble de mesures et précautions lorsque prend fin une relation ou une situation familiale ou parentale fondant le droit d'une personne d'accéder à un espace santé d'une personne.

Il y a des enjeux associés au fait que des proches peuvent accéder à l'espace santé d'un patient, parents pour leurs enfants, accès des personnes aidantes (aidants naturels)

Au plan du *partage patient-médecin*, il y a des enjeux importants concernant la communication et le délai de transfert des informations entre le patient et le médecin. Est-ce que les données envoyées

ont été enregistrées dans le dossier médical? Comment le patient est-il informé que le médecin ou l'équipe de soins a reçu l'information qu'il lui a transmis?

Est-ce qu'il existe un mécanisme de notification signalant que quelqu'un a vu l'information?

L'une des préoccupations d'un patient est de savoir si le médecin ou l'équipe de soins a bien reçu ou vu les données qu'il a envoyées et s'il confirmera la réception.

Or, il importe de préciser, entre l'usager et les professionnels concernés, les conditions dans lesquelles les informations versées dans l'ESP sont effectivement vues et considérées par le professionnel de la santé.

Il faut que les conditions du fonctionnement de l'ESP apportent des réponses à des questions telles que : Quand le médecin verra l'information? Le patient recevra-t-il une réponse? Quand? Les données fournies par le patient ont-elles été prises en compte par le médecin?

Qu'en est-il du délai de transmission des données? Le délai de transmission des données vers le compte de l'utilisateur varie selon le médecin puisque c'est lui qui doit examiner les données devant être transférées, certains transferts exigeant plus de temps que d'autres. Des risques réels existent pour l'information qui n'a pas été reçue ou revue à temps et celle qui requiert une réponse urgente doivent être considérés et donner lieu à une ligne de conduite claire et raisonnable.

Les responsabilités

L'ESP est un espace de partage d'informations. Le participant-patient et le médecin y accomplissent les principales activités. Ils ont leurs responsabilités respectives mais d'autres acteurs, procurant l'environnement technique de communication peuvent aussi avoir certaines responsabilités.

Le patient

Le patient dispose du plein contrôle sur les documents qu'il décide de mettre dans son espace santé personnel. Il est le seul à avoir la maîtrise, le contrôle de ce qui entre, sort et demeure dans son espace.

Il est donc important qu'il soit informé et qu'il soit en mesure de prendre conscience des risques de partager avec des tiers des informations sur son dossier médical, son DSQ de même que d'autres informations sur son état de santé.

Étant donné le haut degré de sensibilité des informations concernées, il n'est pas excessif d'exiger que des mesures adaptées aux niveaux cognitifs des différents usagers soient mises en place afin de les informer adéquatement et de façon significative des enjeux et risques inhérents à un partage tel que celui que permet l'ESP.

La maîtrise par le participant concerne aussi bien la production d'information que les interactions qui prennent place à l'occasion de divers évènements. Selon le type d'activités auxquelles s'adonne le participant, diverses règles pourront trouver application. Il lui incombe donc de connaître et de gérer les divers types d'enjeux et risques inhérents aux activités qu'il mène dans son espace santé personnel.

Le participant a l'obligation de protéger l'ensemble des éléments qui lui permettent de s'identifier dans le système. Il a le devoir de tenir à jour les informations qui le concernent et l'obligation de signaler la perte de l'identifiant car cela entraine la compromission possible du certificat.

Compte tenu du haut degré de maîtrise qu'il exerce, le participant a l'obligation d'évaluer les enjeux et d'activer les configurations qui réservent à des catégories de personnes déterminées, la faculté d'accéder et de consulter certains documents. Si le titulaire de l'ESP néglige d'effectuer de telles configurations, il pourra avoir à subir les conséquences qui pourraient en découler.

Le médecin

Dans l'environnement de partage tel que l'ESP, les responsabilités du médecin ne sont pas diminuées. Elles prennent toutefois de nouvelles dimensions.

Ainsi, l'obligation de suivre et d'informer requiert que le médecin précise les situations où l'ESP ne peut être utilisé, lorsqu'il y a un problème de santé urgent ou qui exige une réponse rapide ou une orientation vers d'autres ressources.

Il faut informer le patient des risques d'avoir recours aux communications électroniques pour discuter de renseignements de santé de nature délicate.

L'information nécessaire à un consentement libre et éclairé du patient doit inclure ce qui concerne les moyens de télécommunication utilisés, dont :

- Les limites de l'exercice médical compte tenu des moyens de communication utilisés;
- Les bris possibles de confidentialité liés aux moyens de communication utilisés;
- La conservation de renseignements sur support électronique

Ces aspects du consentement doivent être documentés au dossier du patient.

C'est la clinique ou le professionnel de la santé qui est engagé dans une relation de soins qui est le mieux en mesure d'informer le patient des avantages mais aussi des enjeux et risques inhérents à l'ESP.

En particulier, il faut que le patient soit clairement et complètement informé des enjeux et risques inhérents au partage des informations de son ESP avec les tiers qu'il autorise.

Il appartient au médecin d'évaluer si les technologies de l'information utilisées pour communiquer avec son patient permettent de préserver le secret professionnel. S'il utilise l'ESP pour partager de l'information avec son patient, le médecin a le devoir d'informer le patient des limites de cette technologie non seulement en terme de communication (délai de réponse…) mais également relativement à la confidentialité des échanges

La transmission d'information issue des dossiers médicaux doit emprunter des moyens protégeant la confidentialité de ces informations.

Les informations et les conseils donnés au médecin au moyen des technologies de l'information, qu'ils proviennent du patient ou d'un membre de l'équipe de soins doivent être consignés au dossier du patient. Cela inclut tous les courriels et textos envoyés ou reçus.

Lorsque des paramètres biologiques et des données de monitorage sont fournis au médecin par son patient (glycémie, prise de tension artérielle) ou par des tiers, le médecin doit documenter dans le

dossier du patient la technologie utilisée et les conditions définies avec le patient afin de s'assurer de la validité de ces paramètres.

L'ESP doit présenter des fonctionnalités permettant l'identification de tous les utilisateurs et la journalisation des accès au document et garantir l'inaltérabilité des transactions («toute transaction doit être enregistrée, ne peut être modifiée lorsque signée et les modifications subséquentes doivent être «retraçables»).

Un médecin qui assure le suivi de plusieurs membres d'une même famille doit être extrêmement vigilant et doit protéger le secret professionnel envers chacun des membres du couple ou de la famille.

En cas de séparation des conjoints ou autres modifications des relations familiales, se posent forcément d'importants enjeux quant à la discontinuation des droits d'accès à l'espace santé par un ancien conjoint ou par une personne à laquelle le titulaire de l'ESP souhaite retirer les droits qu'elle s'était vue conférer sur son espace santé.

Si a priori, la responsabilité d'agir dans de telles situations incombe au patient titulaire de l'ESP, il est impossible d'exclure complètement la responsabilité du médecin en de pareilles circonstances dans lesquelles le partage avec un tiers est autorisé.

Le prestataire de service

Même s'il ne peut exercer le contrôle sur les documents consignés dans l'ESP, le prestataire de service assume un certain nombre de responsabilités.

En vertu de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire de service a une obligation générale de protéger la sécurité, l'intégrité et la confidentialité des documents placés par les usagers dans les espaces santé personnels

Le prestataire du service n'est pas tenu de surveiller l'information ni de rechercher des circonstances qui pourraient indiquer que des documents permettent la réalisation d'activités illicites.

Le prestataire du service n'a pas le droit de surveiller. Tant les règles générales sur le droit à la vie privée que les impératifs de secret inhérents à la relation de soins de santé s'opposent à ce qu'un tiers qui n'est pas impliqué dans la relation de soins puisse prendre connaissance des informations qui sont consignés dans les environnements qui permettent le fonctionnement de l'espace santé personnel.

Les fournisseurs d'applications logicielles

L'utilisation par un usager d'applications logicielles branchées à l'espace TELUS pour collecter et stocker des données dans son espace personnel pourrait soulève certains enjeux. Il faut en particulier porter attention à ce qu'il advient des informations collectées à partir de l'outil médical connecté à un ESP. Ces risques sont habituellement divulgués au niveau de l'outil médical connecté mais il subsiste la question de l'effet cumulatif du raccordement de l'ESP à un ensemble d'outils médicaux connectés. Les conditions du traitement des informations recueillies à partir des outils médicaux et conservés par les serveurs associés à de tels outils soulèvent aussi des enjeux. Des risques significatifs sont associés à la circulation d'information et à la possible perte de confidentialité de renseignements sensibles.