L'intégration de la confidentialité dans la conception des dossiers de santé électroniques pour permettre de multiples fonctionnalités : une situation où tout le monde gagne

2 MARS 2012

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Canada Health Infoway
Inforoute Santé du Canada

Ann Cavoukian, Ph.D.
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Richard C. Alvarez, ICD.D
Président et chef de la direction
Inforoute Santé du Canada

Inforoute Santé du Canada
1000, rue Sherbrooke Ouest
Bureau 1200
Montréal (Québec) H3A 3G4
Site Web : www.inforway-inforoute.ca

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

Cette publication est disponible sur le site Web du Bureau du commissaire.

This publication is also available in English.

L'INTÉGRATION DE LA CONFIDENTIALITÉ DANS LA CONCEPTION DES DOSSIERS DE SANTÉ ÉLECTRONIQUES POUR PERMETTRE DE MULTIPLES FONCTIONNALITÉS : UNE SITUATION OÙ TOUT LE MONDE GAGNE

par
Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario
et
Richard C. Alvarez, ICD.D, président et chef de la direction, Inforoute Santé du Canada

Introduction

Les renseignements personnels sur la santé regroupent certaines des informations les plus intimes sur la vie d'une personne, par exemple celles qui ont trait à son état physique ou mental, ou encore à ses antécédents familiaux. Il faut donc les assujettir à de solides sauvegardes si l'on veut en préserver la confidentialité. Ces renseignements doivent aussi être exacts, complets et accessibles aux prestateurs de soins. Par ailleurs, les renseignements sur la santé ont depuis longtemps des utilisations secondaires d'une valeur inestimable, qui vont au-delà des soins et traitements offerts à la personne et qui sont jugés profitables à l'ensemble de la société. Ils servent, par exemple, à des fins aussi variées que la surveillance de la santé de la population, l'amélioration de la qualité, la recherche en santé et la gestion du réseau de santé public du Canada.

Plus le recours à des technologies informatiques comme les dossiers de santé électroniques (les DSE) se répand dans ce secteur, plus il devient difficile de conjuguer l'obligation de confidentialité avec les avantages dont peuvent s'assortir les utilisations secondaires. S'il demeure important de maximiser les deux, les progrès technologiques qui donnent lieu à des utilisations plus rapides, plus exactes et moins coûteuses des renseignements personnels sur la santé posent de nouveaux défis au chapitre de la confidentialité, de la sécurité et de la transparence. D'une part, le passage des dossiers papier aux dossiers électroniques permet un accès immédiat à de grands volumes de renseignements personnels sur la santé, souvent à de grandes distances, ce qui peut améliorer énormément les soins primaires et favoriser les utilisations secondaires. D'autre part, les systèmes électroniques posent des risques uniques pour la confidentialité et la sécurité des renseignements, notamment et surtout parce que des renseignements peuvent être recueillis auprès de sources diversifiées et consultés à l'ordinateur par des utilisateurs autorisés situés à des milliers de kilomètres du lieu original de la collecte. Les renseignements entreposés indéfiniment dans de vastes dépôts de données peuvent être facilement et plus rapidement reliés à ceux d'autres dépôts du même genre et sont susceptibles d'être utilisés à des fins de plus en plus nombreuses – et nouvelles.

Le passage des dossiers papier aux DSE soulève certaines questions en ce qui a trait aux utilisations secondaires. Qui décidera de ces utilisations? Comment? Quelles mesures existent ou devraient être en place pour favoriser la confidentialité et la sécurité des dossiers? Comment promouvoir la transparence des utilisations et des divulgations? Comment maintenir la confiance du public envers la capacité des systèmes électroniques de préserver la confidentialité compte tenu, en particulier, de la croissance des DSE et de la possible expansion des utilisations secondaires? Si le public craint que ces systèmes ne parviennent pas à sauvegarder les renseignements personnels les plus délicats, nous pourrions être privés d'une source d'information de qualité, essentielle non seulement pour les utilisations secondaires vitales, mais – plus important encore – pour les utilisations primaires qui contribuent à maintenir notre population en bonne santé et en sécurité.

Nous commencerons par une analyse de certains des éléments, déjà en place ou en voie d'être établis, qui constituent le fondement d'une structure de gouvernance des utilisations secondaires des DSE. Il s'agit notamment des exigences légales, de la surveillance indépendante de la confidentialité et des principes établis dans le *Recueil des notions communes* rédigé par une entité pancanadienne, le Groupe de protection des renseignements personnels sur la santé. Nous préconisons le maintien de l'utilisation secondaire des renseignements contenus dans les DSE, comme cela se faisait pour les dossiers papier, d'une façon qui respecte à la fois les droits d'une personne à leur confidentialité et les intérêts sociaux en général.

Nous préconisons, dans le contexte des DSE, une approche des utilisations secondaires qui fait sienne la *Protection intégrée de la vie privée* (PIVP). La PIVP non seulement satisfait aux valeurs de la confidentialité des renseignements personnels, mais renforce de fait leur protection et contribue ainsi à en garantir l'accès pour des utilisations secondaires qui profitent à tout le monde. Cette approche repose sur le principe implicite suivant : les renseignements devraient être automatiquement anonymisés et être utilisés et divulgués comme tels à des fins secondaires, et s'il devait s'avérer que les renseignements anonymisés ne permettent pas d'arriver aux fins escomptées, des sauvegardes additionnelles devraient alors être mises en place avant que les renseignements personnels sur la santé puissent être utilisés et divulgués. Dans le présent document, une distinction est faite entre les renseignements personnels sur la santé, qui concernent la santé et la prestation de soins à une personne, et l'information sur la santé, qui désigne des renseignements anonymisés.

La valeur de l'information électronique sur la santé pour la recherche et les utilisations du réseau de santé

Tout le monde est familiarisé avec certaines utilisations courantes des renseignements personnels sur la santé à des fins autres que les soins directs et les traitements administrés à une personne, par exemple le traitement des demandes, l'amélioration de la qualité et la recherche en santé. Les lois sur la protection des renseignements personnels reconnaissent la valeur de ces utilisations et permettent généralement la collecte, l'utilisation et la divulgation des renseignements personnels, y compris ceux qui concernent la santé, à des fins secondaires dans certaines circonstances. En Ontario, par exemple, la *Loi sur la protection des renseignements personnels sur la santé* de 2004 (la LPRPS) pose des règles claires à cet égard.

La valeur inestimable des utilisations secondaires a aussi été soulignée dans le rapport publié en octobre 2002 par le comité sénatorial présidé par Michael Kirby, qui était chargé d'examiner l'état du système de santé au Canada [« le rapport

Kirby »][1] ainsi que dans le rapport d'une commission présidée par Roy J. Romanow sur l'avenir du réseau de santé à financement public du Canada, en novembre 2002 [« le rapport Romanow »][2]. Ces rapports reconnaissaient l'importance des rôles multiples que jouent les utilisations secondaires : par exemple, elles nous aident à mieux comprendre les déterminants de la santé, à créer des directives concernant la pratique clinique et à améliorer celles qui existent déjà, à cerner des façons de rentabiliser les activités du réseau de santé, à faciliter les activités de promotion de la santé et de prévention des maladies, à mesurer les besoins en services de santé, à surveiller et évaluer les services pour allouer efficacement les ressources et, enfin, à renseigner les citoyens sur les mesures qu'ils peuvent prendre d'emblée pour améliorer leur santé en général. Ils reconnaissaient aussi que les renseignements recueillis dans un réseau de santé à financement public pouvaient et devaient contribuer au bien public et être utilisés au profit de la santé des Canadiens en général.

De même, les rapports Kirby et Romanow reconnaissent explicitement le rôle joué par la technologie des soins de santé, et plus précisément les DSE, dans l'accès aux renseignements à des fins de recherche et d'utilisation secondaire connexe[3]. Les utilisations primaires et secondaires profitent de l'adoption répandue des systèmes faisant appel aux DSE, qui offrent maints avantages sur les dossiers de papier traditionnels archivés par les prestateurs de soins. En effet, les dossiers de santé conservés sous forme électronique exigent moins d'espace, et il faut moins de ressources pour en assurer l'administration. De plus, ils peuvent être partagés et consultés facilement par toutes les parties prenantes aux soins de santé d'une personne, sans égard à l'endroit où elles se trouvent. Enfin, ces dossiers sont plus susceptibles de renfermer des renseignements complets et à jour sur la santé du patient.

Lorsque des systèmes de DSE sont construits en fonction de normes d'encodage et de messagerie uniformes à l'échelle pancanadienne, ils peuvent être mis à profit pour étayer des études qui concernent l'ensemble du pays. L'uniformité des normes de ce genre – et d'autres normes architecturales – est au cœur même du travail d'Inforoute Santé du Canada. Cet organisme à but non lucratif financé par le gouvernement fédéral et chargé de coordonner l'élaboration et le déploiement de DSE interexploitables au Canada reconnaît la nécessité d'accéder à des renseignements sur la santé longitudinaux exacts et fiables à des fins de recherche, d'analyses et pour d'autres utilisations. Grâce à son architecture conceptuelle de confidentialité et de sécurité, il est en mesure de favoriser l'intégration, dans tous

1 SÉNAT DU CANADA, Comité sénatorial permanent des Affaires sociales, de la science et de la technologie, *La santé des Canadiens – Le rôle du gouvernement fédéral, rapport final sur l'état du système de soins de santé au Canada, Volume six : Recommandations en vue d'une réforme, Chapitre 10 : Le rôle du gouvernement fédéral dans l'infrastructure de soins de santé*, (Ottawa, octobre 2002) (Président : Michael Kirby) [« Le rapport Kirby »].

2 CANADA, CONSEIL PRIVÉ, Commission sur l'avenir des soins de santé au Canada, *Guidé par nos valeurs : L'avenir des soins de santé au Canada, Rapport final* (Ottawa, novembre 2002) (Commissaire Roy J. Romanow, c.r.) [« Le rapport Romanow »].

3 V. Rapport Kirby, *supra*, note 1, pp. 183-198; Rapport Romanow, *supra*, note 2, Chapitre 3: L'information, les données, les idées, pp. 81-98.

les systèmes de DSE, de solides caractéristiques de sécurité et de confidentialité comme le chiffrement et l'anonymisation des données[4].

À mesure qu'avance la mise en place des systèmes électroniques dans le réseau de la santé, nous pouvons clairement commencer à observer les avantages cliniques du regroupement électronique des renseignements personnels sur la santé. En Ontario, par exemple, à Sault Ste. Marie, un projet pour lequel Inforoute Santé du Canada a donné son soutien mettait en relation les médecins et pharmaciens qui participaient au traitement de patients atteints de maladies chroniques en procurant aux pharmaciens de la localité un accès aux dossiers médicaux électroniques tenus par les cabinets des médecins. Grâce à cet accès commun, le projet, baptisé « DMExtra », permet d'améliorer la qualité des soins offerts aux malades chroniques, en plus de susciter beaucoup plus de satisfaction de part et d'autre. Parmi les avantages cliniques mesurables qui ont été observés, mentionnons un meilleur dépistage des problèmes attribuables aux médicaments, l'engagement plus actif auprès des patients signalé par les pharmaciens, une pharmacothérapie mieux coordonnée grâce à la diminution des erreurs dans la liste des médicaments, ainsi qu'une plus grande autonomie et une meilleure habilitation des patients, de l'aveu même de ceux-ci[5].

Outre les avantages cliniques, les systèmes électroniques ont le potentiel de faciliter les utilisations secondaires. En leur absence, les renseignements personnels sur la santé sont encore souvent conservés en format papier et sous des formes disparates par chacun des prestateurs de soins, et même lorsqu'ils ont été numérisés, ils sont souvent archivés dans des systèmes locaux qui ne sont pas interopérables. Pour être en mesure de les mettre à profit dans des utilisations secondaires, il faut soit en résumer les données à partir de tableaux en format papier, soit les transférer électroniquement dans des systèmes centralisés. Une fois reçus, les renseignements doivent être traduits en un format standard avant qu'on puisse les relier, les anonymiser et les analyser.

À l'heure actuelle, chaque prestateur de soins de santé agit comme gardien des renseignements personnels sur la santé et a le loisir de déterminer qui peut y avoir accès et à quelles fins. Le commissaire à l'information et à la protection de la vie privée de l'Ontario a observé que lorsqu'un prestateurs de soins de santé décide de divulguer les renseignements ou de les utiliser à des fins secondaires, les renseignements en question demeurent identifiables même si leur anonymisation ne nuit en rien à leur utilisation, simplement parce qu'il n'a pas les ressources ou la capacité de les anonymiser au préalable. Et même s'il était en mesure de le faire, l'accès à des renseignements non anonymisés est souvent nécessaire lorsqu'il faut relier des renseignements qui datent ou qui proviennent de sources disparates pour les rendre aptes à servir pour des utilisations secondaires.

4 Inforoute Santé du Canada, *Vue d'ensemble de l'Architecture conceptuelle de confidentialité et de sécurité du dossier de santé électronique (DSE),* Accessible sur le web à l'adresse suivante : https://knowledge.infoway-inforoute.ca/EHRSRA/doc/Architecture-PVPS-Vue-d-ensemble.pdf.

5 INFOROUTE SANTÉ DU CANADA, « Plein feu sur les résultats : DMExtra », 3 mai 2010. Cette histoire de réussite et d'autres comptes rendus du même genre peuvent être consultés sur le site Web d'Inforoute Santé du Canada, à l'adresse suivante : https://www.infoway-inforoute.ca/lang-fr/about-ehr/ehr-success-stories/.

À l'inverse, les DSE peuvent rendre les utilisations secondaires beaucoup plus sûres, bien moins onéreuses et mieux ciblées en éliminant, par exemple, la nécessité de numériser des dossiers papier pour pouvoir les analyser, en facilitant l'anonymisation des renseignements personnels sur la santé et en permettant la création de dépôts où les renseignements sont, *après avoir été anonymisés*, consignés à des fins de recherche et d'analyse. Les transferts par voie électronique favorisent également l'élimination des risques associés à l'acheminement de dossiers papier contenant des renseignements personnels, qui a été à la source de graves atteintes à la confidentialité au cours des dernières années[6],[7].

Les systèmes électroniques permettent aussi d'accélérer et de rendre plus efficientes la recherche et d'autres utilisations secondaires, en automatisant la collecte, l'extraction et l'organisation des données courantes des divers dépôts du DSE. De plus, le DSE peut permettre d'identifier de façon plus confidentielle les participants éventuels à une recherche en automatisant le dépistage initial dans un ou plusieurs champs diagnostiques, réduisant par le fait même la nécessité d'une sélection manuelle des dossiers des patients par des personnes qui ne font pas partie de l'équipe de soignants[8]. Ce genre d'automatisation peut améliorer énormément la protection de la confidentialité tout en rationalisant le processus de recherche. De plus, les systèmes électroniques permettent de retracer les données et de les utiliser aisément pour la recherche et l'analyse inhérentes à l'assurance de la qualité, aux études épidémiologiques et à la surveillance des maladies.

Nous le répétons, l'établissement d'une architecture et de normes communes pour les données recueillies partout au pays a été l'une des plus importantes caractéristiques de la démarche adoptée par Inforoute Santé du Canada pour la création des DSE. Plus la normalisation et l'intégration gagneront du terrain, plus l'interopérabilité et le partage autorisé des renseignements dans tous les systèmes et dans chaque province et chaque territoire seront faciles. Les systèmes de DSE adoptés par chaque administration peuvent permettre l'établissement de dépôts de données grâce auxquels on pourra héberger, administrer et divulguer les renseignements pour des utilisations secondaires. À leur tour, ces dépôts locaux peuvent devenir des plateformes pour des recherches futures, lesquelles

6 On n'a qu'à penser, par exemple, à l'enquête menée par le commissaire à l'information et à la vie privée de la Saskatchewan au sujet de la découverte, dans un bac de recyclage à Regina, de plus de 180 000 dossiers contenant des renseignements personnels sur la santé. Dans un rapport d'enquête publié en juillet 2011, le commissaire a qualifié cet incident de pire atteinte à la confidentialité des renseignements sur les patients depuis la promulgation de la loi concernant l'information sur la santé dans cette province.

7 Le Commissaire à l'information et à la protection de la vie privée de l'Ontario a également publié une série d'ordonnances sur des infractions à la confidentialité survenues au cours de l'acheminement ou de l'élimination de dossiers papier; il s'agit notamment des ordonnances HO-011 (qui concernait la livraison par messager non confirmée de rapports de dépistage du cancer chez plus de 7 000 Ontariens), HO-006 et HO-001 (au sujet de dossiers contenant des renseignements personnels sur la santé trouvés éparpillés dans la rue) et HO-003 (touchant des dossiers abandonnés par une clinique médicale sans rendez-vous au moment de sa fermeture définitive).

8 WILLISON, D., *Utilisation des données du dossier de santé électronique pour la recherche en santé - défis en matière de gouvernance et approches possibles*, mars 2009 [« Willison »], p. 2. Accessible sur le web à l'adresse suivante : http://www.priv.gc.ca/information/pub/ehr_200903_f.cfm.p 2.

serviront à leur tour de sources de données pour une foule de projets de recherche subséquents[9].

En même temps, les avantages inhérents à l'entreposage de quantités massives de renseignements électroniques et la facilité avec laquelle ceux-ci peuvent être reliés pour des utilisations autorisées représentent d'énormes défis au chapitre de la confidentialité et de la sécurité et peuvent compromettre à eux seuls l'acceptation générale des DSE par le public. Il est en outre manifeste que même si le secteur de la santé est tout à fait conscient de la nécessité des utilisations secondaires des DSE, les Canadiens « ordinaires » ne sont pas familiarisés avec le concept. Si l'on veut garantir l'accessibilité continue aux données des DSE pour des utilisations secondaires, il est important de maintenir la confiance du public envers les DSE. Pour ce faire, nous devons corriger les menaces éventuelles à la confidentialité communément associées à la multiplication des utilisations secondaires.

Les difficultés associées aux utilisations par les chercheurs et le réseau de santé des données contenues dans les DSE

Les utilisations secondaires posent des difficultés en ce qui concerne l'adhésion à des principes reconnus de divulgation des renseignements, à commencer par l'idée selon laquelle les renseignements personnels sur la santé ne devraient être recueillis, utilisés et divulgués qu'avec le consentement de la personne concernée. Comme ces renseignements ne sont généralement recueillis qu'au moment de lui fournir des soins, souvent sur la foi d'un consentement implicite, il peut être difficile d'obtenir son consentement éclairé à leur utilisation et à leur divulgation à des fins secondaires, parfois des années après leur collecte. Les mesures de sauvegarde, comme l'anonymisation de ces renseignements et la transparence au sujet de leurs utilisations secondaires, revêtent donc une importance critique. Toute structure d'administration des utilisations secondaires doit s'attacher aux difficultés associées à la sauvegarde des informations contenues dans les DSE.

Difficultés inhérentes à l'anonymisation

Les renseignements personnels sur la santé sont par nature extrêmement délicats, et leur vol, leur perte ou leur divulgation et leur utilisation non autorisées peuvent avoir de lourdes conséquences pour les personnes concernées : discrimination, stigmatisation, troubles psychologiques ou difficultés financières. C'est la raison pour laquelle les bonnes pratiques en cette matière exigent une sélection rigoureuse des occasions où leur collecte est permise; ainsi, on évitera de les recueillir, de

9 KOSSEIM, P. et M. BRADY, « Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes », *Revue de droit et santé de McGill*, 2008 [« Kosseim »], p. 17.

les utiliser ou de les divulguer si d'autres renseignements peuvent servir les fins voulues ou s'il n'est pas absolument nécessaire de le faire.

S'il est clairement nécessaire de pouvoir compter sur des renseignements non anonymes pour assurer la prestation de soins à une personne, il est plutôt rare que ce le soit pour des utilisations secondaires. L'anonymisation devrait donc être implicite et se faire de façon routinière avant l'utilisation ou la divulgation à des fins secondaires. Dans la mesure où les renseignements anonymisés peuvent faire l'objet d'une utilisation secondaire, les risques d'atteinte à la confidentialité deviennent nettement moins élevés. Le passage aux DSE présente de nouvelles occasions d'intégrer directement l'anonymisation dans les méthodes et systèmes, en conformité avec la PIVP.

Même si les DSE faciliteront l'anonymisation des données, l'amélioration de la qualité des renseignements accessibles au moyen des systèmes électroniques peut accroître à son tour les risques de ré-identification. Certains chercheurs ont découvert qu'il est parfois possible de ré-identifier une personne à partir de données apparemment anonymes[10]. Cependant, contrairement aux allégations des détracteurs concernant la possibilité de ré-identification, des études ont révélé que la ré-identification de renseignements adéquatement anonymisés n'est pas une tâche facile – bien au contraire[11]. De plus, elle exige des connaissances spécialisées et une intention bien arrêtée. Si l'anonymisation ne peut garantir l'élimination totale de tous les risques d'atteinte à la confidentialité (à vrai dire, aucun outil ne le pourrait), elle demeure une première étape vitale, qui permet de réduire de façon draconienne le risque d'utilisation ou de divulgation non autorisée de renseignements personnels.

Le recours à des outils d'anonymisation adéquats et à des techniques de mesure des risques de ré-identification (comme ceux dont nous avons brièvement parlé un peu plus haut) reflète une approche de PIVP au défi que représente la protection de la confidentialité tout en permettant l'accès à des renseignements de qualité pour des utilisations secondaires critiques. Lorsqu'elle est faite adéquatement, l'anonymisation demeure l'un de nos meilleurs outils pour offrir ce que nous appelons une réaction de « mégaconfidentialité » aux « mégadonnées », lorsque la puissance toujours plus grande des ordinateurs et l'accessibilité toujours plus grande aux informations facilitent la saisie, la communication, la fusion, l'entreposage et l'analyse d'énormes ensembles de données. Nous reviendrons un peu plus loin à l'anonymisation et à d'autres éléments de l'établissement de la mégaconfidentialité en réaction aux mégadonnées.

10 Voir, par exemple, OHM, Paul, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization » et autres, cités dans CAVOUKIAN, A. et K. EL EMAM, « Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy », juin 2011 [« Dispelling the Myths Surrounding De-identification »]. Accessible sur le web (en anglais seulement) à l'adresse suivante : http://www.ipc.on.ca/images/Resources/anonymization.pdf.

11 El Emam, K, et coll. « A Systemic Review of Re-Identification Attacks on Health Data », document présenté pour publication en 2011, cité dans [« Dispelling the Myths Surrounding De-identification », *supra*, note 10.

Accès non autorisé

À mesure que s'élargit l'accès aux renseignements pour les utilisations secondaires des DSE, il pourrait selon d'aucuns devenir plus difficile de maîtriser le problème actuel d'utilisation et de divulgation non autorisées des renseignements personnels sur la santé contenus dans les DSE par des personnes qui y ont accès. Si la vaste majorité des centaines de milliers d'opérations de DSE qui se déroulent chaque jour a des visées tout à fait légales, des violations de la confidentialité peuvent survenir en raison de prestateurs autorisés de soins de santé qui ont des privilèges d'accès de par leur rôle et qui consultent des dossiers électroniques pour des motifs autres que la prestation de soins de santé. Ce type d'accès inadéquat peut être motivé par des intérêts financiers (comme dans les cas de fraude, de facturation inadéquate ou de vol d'identité), par la curiosité ou par des préoccupations concernant la santé de membres de la famille, de voisins, de collègues ou de célébrités; il peut en outre compromettre sérieusement la réputation institutionnelle et, s'il est porté à la connaissance du public, amener celui-ci à se méfier de la capacité des DSE à protéger la confidentialité.

L'accès sans autorisation n'est pas l'apanage des prestateurs de soins : des utilisateurs secondaires autorisés, par exemple des chercheurs du domaine de la santé, peuvent aussi s'y adonner. Il convient toutefois de souligner que, dans ce cas précis, la transition vers les systèmes électroniques peut en fait contribuer à atténuer le risque d'accès sans autorisation puisqu'il sera relativement facile d'anonymiser les renseignements personnels sur la santé avant qu'ils ne soient utilisés à des fins secondaires. De plus, chaque opération effectuée dans le système est enregistrée et sujette à vérification : la détection de toute activité illicite s'en trouve donc grandement facilitée. Conjuguée à une politique de tolérance zéro, ces pratiques peuvent réduire de façon marquée les activités illicites[12].

La gouvernance des données

Une autre question doit être abordée en ce qui touche les utilisations secondaires : la gouvernance des données. Si, à l'heure actuelle, les prestateurs de soins de santé exercent un contrôle sur leurs propres dossiers papier et électroniques, ils auront plus de difficulté à en exercer un sur les personnes qui y accèdent et sur les raisons pour lesquelles elles le font une fois que le partage des DSE sera devenu chose courante. On pourrait alléguer qu'il vaudrait mieux laisser

12 Aux États-Unis, un médecin de famille rattaché à un important groupe comptant 200 médecins dans 75 cabinets répartis dans deux États a mis en place une politique de tolérance zéro pour les médecins et le personnel qui accèdent de façon illicite aux renseignements personnels sur la santé des patients contenus dans les DME utilisés par le groupe. Le système de DME est hébergé dans un centre de données qui exige que le personnel passe par de multiples étapes d'identification pour accéder aux renseignements voulus; de plus, le système est construit de telle façon qu'il effectue la surveillance en temps réel de l'accès aux serveurs, et tous les accès aux DME par les médecins et le personnel sont portés dans un registre pour vérification. Ces mesures de sauvegarde et la politique de tolérance zéro appliquée dans la pratique ont permis de détecter des accès illicites et d'empêcher qu'ils se reproduisent. Comme le signalait le Commissaire à l'information et à la protection de la vie privée de l'Ontario, le nombre d'infractions est passé de 11 pour l'année où la politique de tolérance zéro a été instaurée à deux l'année suivante. Depuis, le groupe de praticiens congédie de deux à quatre employés chaque année en raison de la politique de tolérance zéro.

ce contrôle entre les mains de chaque prestateur de soins parce qu'il est le mieux placé pour comprendre les souhaits de ses patients et qu'il agit dans leur intérêt. Par contre, on pourrait arguer que ce pouvoir discrétionnaire revenait jusqu'à présent aux prestateurs de soins et qu'il en a résulté des pratiques peu uniformes, tandis que des utilisations secondaires valables étaient freinées par un accès à des renseignements incomplets. Nous reviendrons à la gouvernance des données lorsque nous aborderons un projet de structure plus loin dans le présent document.

La nécessité de la transparence

Malgré les campagnes de sensibilisation publiques, comme la campagne « Vaut mieux savoir » qu'a lancée Inforoute Santé du Canada pour informer les Canadiens au sujet du plan de mise en place des DSE au Canada et des progrès réalisés jusque-là[13], le public ne comprend pas encore très bien comment les renseignements personnels sur la santé sont utilisés et divulgués dans le secteur de la santé, particulièrement dans le contexte des DSE. S'il est vrai que le sujet des utilisations secondaires est complexe, les administrations doivent faire preuve d'ouverture et de transparence lorsqu'il est question de la manière dont les données des DSE seront utilisées à des fins secondaires. Le moindre manquement à la transparence risque d'éroder la confiance du public envers les DSE.

Heureusement, des études révèlent que les Canadiens jugent en général important et précieux le recours aux renseignements des DSE pour certaines utilisations secondaires; ils ne sont pas contre l'idée pourvu que des protections soient mises en place pour en garantir la confidentialité et la sécurité. Par exemple, un sondage réalisé conjointement en 2007 par Inforoute Santé du Canada et le Commissariat à la protection de la vie privée du Canada[14] a révélé que, si la sensibilisation et l'appui aux DSE étaient élevés et augmentaient encore[15], les gens qui s'opposaient à leur développement fondaient leurs objections presque entièrement sur la crainte que les renseignements personnels sur la santé qui y sont consignés ne soient pas adéquatement protégés[16]. L'application préconisée de certaines mesures, par exemple l'instauration de pistes de vérification, l'imposition de lourdes sanctions pour un accès sans autorisation et la publication des infractions à la confidentialité calment quelque peu leurs inquiétudes.

---

13 Voir le microsite de la campagne de sensibilisation publique d'Inforoute Santé du Canada à l'adresse suivante : www.vautmieuxsavoir.ca.

14 LES ASSOCIÉS DE RECHERCHE EKOS, *Sondage sur les renseignements de santé électroniques et la protection de la vie privée : Le point de vue des Canadiens — 2007*, août 2007 [« Le sondage EKOS 2007 »]. Accessible sur le web à l'adresse suivante : https://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_FR.pdf.

15 Sondage EKOS 2007, *supra*, note 14, p. 4 : « Près de la moitié des Canadiens (49 p. 100) disent avoir entendu parler des DSE (résultat témoignant d'une augmentation de huit p. 100 par rapport à 2003). De plus, le tiers des Canadiens (31 p. 100) ont eu une interaction avec un système de cette nature. Dans une proportion de près de neuf pour dix (88 p. 100), les Canadiens appuient la mise au point des DSE (résultat témoignant d'une augmentation de cinq p. 100 par rapport à 2003). »

16 *Ibid.*, p. 47.

De plus, environ les trois quarts des Canadiens sont très favorables à l'idée d'utiliser les DSE pour prévenir une utilisation inadéquate du réseau de santé, pour planifier, surveiller et évaluer les activités qui s'y déroulent, ou pour prévoir des enjeux touchant la santé et y réagir[17]. Plus de huit répondants sur dix (84 %) appuient le recours aux DSE pour la recherche en santé si les renseignements sont anonymisés; le soutien diminue de façon marquée (à 54 %) si des renseignements non anonymisés sont utilisés et n'est qu'à peine plus élevé (à 66 %) si un consentement est fourni au préalable[18]. L'approbation du partage de renseignements anonymisés varie en fonction du destinataire; elle est plus élevée s'il s'agit de gouvernements, de chercheurs, d'organismes de la santé et d'organisations qui recueillent des statistiques que s'il s'agit d'entreprises du secteur privé[19].

Il est primordial de maintenir et de faire croître la confiance du public envers la capacité des systèmes de DSE de préserver la confidentialité. Selon certaines études, les personnes qui s'inquiètent au sujet d'une utilisation inappropriée ou d'une divulgation de leurs renseignements personnels sur la santé peuvent adopter des comportements défensifs, par exemple omettre de donner des renseignements à un prestateur de soins ou encore lui donner des renseignements inexacts, éviter le traitement ou les analyses diagnostiques de certaines affections, même s'ils sont nécessaires, ou choisir de payer certains médicaments et services de leur poche plutôt que de soumettre une demande de remboursement à leur assureur[20]. Ces comportements peuvent mener à la collecte de renseignements incomplets ou inexacts, ce qui peut nuire aux soins et aux utilisations secondaires. Même si le public semble croire à l'importance de certaines utilisations secondaires des renseignements contenus dans les DSE, il faudra maintenir sa confiance envers la capacité des utilisateurs secondaires de protéger ces renseignements si l'on veut continuer d'y avoir accès.

Vers un cadre de gouvernance des utilisations des DSE pour la recherche et le réseau de santé

Examinons maintenant les mesures de protection de la confidentialité qui pourraient être intégrées à un cadre de gouvernance des utilisations secondaires des DSE. Les documents intitulés *Protection intégrée de la vie privée* (PIVP) et *Recueil des notions communes* exposent les principes qui devraient sous-tendre un tel cadre, tout comme les outils et mécanismes déjà accessibles et dont l'usage devrait être plus répandu. D'autres enjeux encore devraient être analysés et débattus par les parties prenantes. C'est donc dire que le cadre ne sera pas statique et

17 *Ibid.*, p. 69.

18 *Ibid.*, p. 71.

19 *Ibid.*, p. 27.

20 CALIFORNIA HEALTHCARE FOUNDATION AND FORRESTER RESEARCH, INC., *National Consumer Health Privacy Survey 2005,* novembre 2005. Accessible sur le web (en anglais seulement) à l'adresse suivante : http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.

qu'il évoluera avec le temps. Malgré cela, il devra protéger la confidentialité des renseignements personnels tout en permettant l'accès à des renseignements de qualité pour les utilisations secondaires critiques. Ce principe est fondé sur la PIVP, qui préconise un modèle de double habilitation à somme positive dans lequel les deux valeurs (la confidentialité et la qualité des données) sont portées à leur maximum.

Protection intégrée de la vie privée

Dans le secteur de la santé, le traditionnel jeu à somme nulle place en opposition la protection des renseignements personnels du patient et l'intérêt général du public (dans ce cas, l'accès à des renseignements sur la santé de grande qualité pour la recherche et d'autres utilisations), ce qui mène à un scénario gagnant-perdant dans lequel l'intérêt d'une partie est inévitablement subordonné à celui de l'autre. La PIVP rejette le paradigme traditionnel à somme nulle et préconise une intégration proactive et implicite de la confidentialité dans la conception même des technologies de l'information, des infrastructures réseautées et des pratiques informatiques; ainsi, non seulement la confidentialité serait-elle une composante essentielle des fonctionnalités de base qui sont établies, mais elle ne « nuirait » pas à la coexistence d'autres fonctionnalités tout aussi importantes.

Nous entrons dans une ère de mégadonnées, et la PIVP offre une approche globale et proactive de la protection de la confidentialité qui peut nous aider à prévoir et à corriger les « mégamenaces » dont s'assortiront selon toute logique les mégadonnées. En même temps, la PIVP reconnaît la nécessité de mettre les mégadonnées au service de la société et travaille à en faire ressortir les avantages. Dans le contexte de la conception et de la mise en place de systèmes de DSE, la PIVP a pour objectif de protéger les renseignements personnels sur la santé contenus dans les DSE tout en répondant à de multiples objectifs : la confidentialité *et* la sécurité, les avantages pour la personne *et* pour la société, la protection *et* la qualité des données. Ainsi, l'accès aux renseignements sur la santé à des fins secondaires en sera facilité, sans pour autant compromettre la confidentialité des renseignements sur la santé contenus dans le DSE. Comment? Par une intégration directe de la confidentialité et de la sécurité dans les systèmes de DSE, par une anonymisation routinière des renseignements personnels sur la santé utilisés à des fins secondaires, ainsi que par certains mécanismes de sécurité de bout en bout et autres dont il est question ailleurs dans le présent document. La PIVP offre un moyen de donner à la confidentialité toute l'importance qu'elle mérite comme contrepoids dans le contexte des mégadonnées; elle est une façon de garantir l'enchâssement de la confidentialité comme condition *primordiale* de toutes les opérations où des mégadonnées sont en jeu. En suivant les paramètres de la PIVP, le Groupe pancanadien de protection des renseignements personnels sur la santé a examiné de façon proactive, dans son document qui décrit les principes généraux de gouvernance de l'information dans le contexte des DSE, les répercussions des utilisations secondaires sur la confidentialité.

Recueil des notions communes pancanadiennes

Dans son premier Recueil des notions communes[21], le Groupe pancanadien de protection des renseignements personnels sur la santé (constitué en décembre 2008 et formé de membres du Forum pancanadien sur la confidentialité – Gouvernance de l'information dans le DSE), a énoncé 33 principes à l'appui d'une divulgation appropriée et confidentielle, entre les administrations, des renseignements contenus dans les DSE. Ces notions communes sont des déclarations consensuelles des membres du Groupe à l'égard des objectifs de promotion de l'uniformité et de contribution aux travaux visant l'encadrement législatif de la confidentialité des dossiers médicaux dans les administrations, les politiques de télésanté connexes, les ententes sur l'échange de renseignements et, enfin, les exigences administratives et techniques des systèmes de DSE[22].

Les principes énoncés dans le *Recueil des notions communes* fournissent une orientation pour la mise au point d'un cadre pratique de gestion des utilisations secondaires dans le contexte des DSE. Outre celles qui portent sur la divulgation, entre les administrations, des traitements et soins de santé et sur l'obligation de reddition de comptes dont s'assortit la gouvernance des DSE interopérables, certaines notions concernent spécifiquement les divulgations interadministrations pour utilisation secondaire[23]. Ces notions communes préconisent les mesures suivantes :

- l'agrégation ou l'anonymisation des renseignements personnels sur la santé doit être une condition *sine qua non* de leur utilisation secondaire;
- des méthodes d'évaluation des risques, des accords sur la divulgation des données, des pratiques de sécurité et d'autres mesures de précaution doivent être mises à contribution pour réduire au minimum les risques inhérents à la divulgation des renseignements pour des utilisations secondaires;
- les patients doivent être avisés de la divulgation des renseignements qui les concernent pour des utilisations secondaires dans une autre administration, et une trace de cette divulgation de renseignements non anonymisés doit être conservée dans les dossiers pour qu'un rapport puisse en être fait à la demande des patients;
- des accords énonçant les obligations et conditions rattachées à la gestion des renseignements sur la santé divulgués à d'autres administrations à des fins secondaires doivent être établis;

21 Inforoute Santé du Canada, Groupe pancanadien de protection des renseignements personnels sur la santé, *La confidentialité et la circulation des données de DSE au Canada : Recueil des notions communes du Groupe pancanadien de protection des renseignements personnels sur la santé,* juin 2010 [« Recueil des notions communes »]. Accessible sur le web à l'adresse suivante : https://www2.infoway-inforoute.ca/Admin/Upload/Dev/Document/Common_Understandings_Privacy_FR.pdf

22 *Recueil des notions communes*, *supra*, note 21, p. 5.

23 *Ibid.*, pp. 22-27.

- les entités et personnes qui traitent les demandes de divulgation inter-administrations de renseignements des DSE à des fins secondaires doivent maîtriser les plus récentes utilisations et applications des outils d'anonymisation; et

- il faut procéder à des délibérations pancanadiennes sur les enjeux des utilisations secondaires et élaborer des recommandations qui seront étudiées par toutes les administrations en vue de promouvoir une approche uniforme de la question dans l'ensemble du pays.

Les principes de la PIVP, de concert avec les Notions communes, doivent servir d'assise pour le cadre dans lequel seront enchâssées les utilisations des renseignements personnels sur la santé par les chercheurs et le réseau de santé, dans le contexte des DSE. En fait, nombre de ces principes ont déjà été intégrés dans les mesures actuelles de protection de la confidentialité dans les utilisations secondaires, comme nous le décrivons ci-dessous.

Les éléments existants d'un cadre de gouvernance des utilisations par les chercheurs et le réseau de santé

Législation, politiques et procédures sur la protection des renseignements personnels

Les provinces et territoires ont tous adopté des mesures législatives pour protéger les renseignements personnels; huit en ont promulgué qui concernent spécifiquement la santé[24]. Ces dispositions législatives autorisent habituellement les utilisations secondaires dans des circonstances précises; les renseignements qui n'ont pas trait à une personne identifiable ne sont pas réputés être visés par les dispositions législatives en question.

Souvent, des règles particulières sont établies pour la recherche. Les dispositions législatives sur la confidentialité dans le secteur de la santé, comme la LPRPS de l'Ontario, permettent la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé à des fins de recherche, dans certains cas sous réserve du consentement de la personne concernée, dans d'autres sans le consentement en question, mais sous réserve du respect d'exigences bien précises. Si les diverses administrations ont des exigences variées quant au caractère détaillé et à la rigueur des obligations, elles imposent généralement la préparation d'un plan de recherche, son approbation par un conseil d'éthique, la mention des points sur lesquels celui-ci doit se pencher pour ce qui concerne la confidentialité avant d'approuver le plan de recherche, et l'obligation, pour les gardiens ou les dépositaires des dossiers, d'être parties prenantes à un accord écrit conclu avec

24 Il s'agit de l'Alberta, de la Colombie-Britannique, du Manitoba, du Nouveau-Brunswick, de Terre-Neuve, de la Nouvelle-Écosse, de l'Ontario et de la Saskatchewan.

les chercheurs si ceux-ci sont mandatés par une tierce partie[25]. Parmi les autres lignes directrices concernant la recherche, mentionnons l'Énoncé de politique des trois conseils sur le Code d'éthique de la recherche avec des êtres humains et le Code type de la CSA, ainsi que les obligations d'ordre légal et professionnel applicables. Dans certaines provinces, des dispositions législatives imposent la création de comités spéciaux de fiducie des données chargés d'administrer la divulgation des renseignements contenus dans les bases de données provinciales à des fins de recherche et de planification de la santé[26].

D'autres protections pourraient devoir être enchâssées dans les lois à mesure que s'élargira l'accès, pour des utilisations secondaires, aux renseignements personnels sur la santé contenus dans les DSE. Par exemple, il peut falloir établir des pouvoirs législatifs clairs pour la prise de décisions concernant leur utilisation et leur divulgation à ces fins puisqu'aucun dépositaire unique ne peut avoir le pouvoir de le faire s'il y a échange du dossier.

Surveillance de la confidentialité

La surveillance indépendante de la confidentialité est un élément important de tout cadre de gouvernance de l'utilisation secondaire des données contenues dans les DSE. Toutes les administrations ont établi des organismes chargés de veiller au respect des lois en cette matière et d'enquêter sur les plaintes. Leurs pouvoirs varient selon l'administration : certaines, comme l'Ontario, leur ont donné le pouvoir de faire des recommandations, d'autres, de rendre des ordonnances.

En Ontario, le commissaire à l'information et à la protection de la vie privée a des pouvoirs d'ordonnance et les a utilisés dans plusieurs cas d'accès sans autorisation à des renseignements personnels sur la santé contenus dans des dossiers électroniques. Par exemple, une ordonnance a été rendue dans le cas d'une infirmière qui a consulté le dossier médical d'une patiente de l'hôpital où elle travaillait et a transmis les renseignements qu'il contenait au mari de la patiente, dont celle-ci était séparée, lui-même un employé de l'hôpital, même si l'infirmière ne participait pas aux soins de la patiente et que celle-ci avait spécifiquement mentionné au moment de son admission ne pas vouloir que ses renseignements soient divulgués[27]. Dans une autre affaire qui a eu lieu par la suite dans le même hôpital, le commissaire a conclu que les efforts déployés par l'administration de l'établissement pour prévenir la consultation et la divulgation

25 INSTITUTS DE RECHERCHE EN SANTÉ DU CANADA (Kosseim, Patricia, dir.), *Recueil des dispositions législatives canadiennes sur la protection des renseignements personnels dans le contexte de la recherche en santé* (Travaux publics et Services gouvernementaux Canada, Ottawa, 2005) pp. 63-64. Accessible sur le web à l'adresse suivante : http://www.cihr-irsc.gc.ca/f/documents/ethics_privacy_compendium_june2005_f.pdf.

26 KOSSEIM, *supra*, note 9, p. 11, citant *l'E-Health (Personal Health Information Access and Protection of Privacy) Act* de la C.-B. Voir aussi la *Health Information Act* de l'Alberta, qui crée un comité provincial de fiducie des données des DSE et le charge de formuler des recommandations sur les règles de consultation, d'utilisation, de divulgation et de conservation des renseignements sur la santé prescrits et accessibles dans les DSE de l'Alberta.

27 Ordonnance HO-002 du commissaire à l'information et à la protection de la vie privée de l'Ontario. Accessible sur le web (en anglais seulement) à l'adresse suivante : http://www.ipc.on.ca/images/Findings/up-HO_002.pdf.

sans autorisation des renseignements personnels sur la santé par les agents et employés de l'hôpital n'avaient pas porté fruit.

Compte tenu de la prolifération des DSE, il pourrait falloir passer en revue les pouvoirs des organismes de surveillance de la confidentialité et les élargir afin d'en garantir l'efficacité pour la surveillance de toutes les utilisations secondaires des renseignements personnels sur la santé.

Architecture de DSE apte à protéger la confidentialité

Nous le répétons, des DSE bien conçus sont plus aptes à protéger la confidentialité que des dossiers papier. Des mesures implicites de sécurité et de sauvegarde de la confidentialité peuvent être intégrées aux systèmes de DSE. L'architecture conceptuelle de confidentialité et de sécurité élaborée par Inforoute Santé du Canada repose sur un ensemble de plus d'une centaine d'exigences à ce titre. L'architecture fait en sorte que les systèmes interopérables des DSE respectent les exigences de confidentialité et de sécurité fédérales, provinciales et territoriales, ainsi que les exigences inter-administrations ayant trait aux soins et traitements de santé et à l'utilisation secondaire. Elle s'assortit de multiples sauvegardes de la confidentialité et de la sécurité qui s'appliquent non seulement aux DSE en général, mais aussi à l'utilisation secondaire des renseignements qu'ils contiennent. Par exemple, les fonctions d'anonymisation référencées dans l'architecture répondent à la nécessité pour les systèmes d'allouer le retrait d'identifiants dans un dossier pour permettre une utilisation secondaire du renseignement; les fonctions de chiffrement répondent à la nécessité de protéger les renseignements lorsqu'ils sont entreposés ou transmis, et les fonctions de vérification de la sécurité garantissent l'enregistrement de toutes les opérations afin de permettre le suivi et le rapport de toutes les utilisations et divulgations à quelque fin que ce soit, y compris les utilisations secondaires.

Il existe aussi des applications qui s'attachent au risque de plus en plus grand représenté par les utilisateurs qui jouissent d'une autorisation d'accès, par exemple les logiciels de prévention de la fraude et de détection des violations de sécurité. Elles peuvent aider à prévenir et à détecter les infractions en enregistrant les tendances au chapitre de l'accès et de l'utilisation des dossiers électroniques, en surveillant et en analysant les comportements des utilisateurs à la recherche de comportements qui pourraient dénoter une utilisation illicite et en générant des alertes ou des signalements visant à freiner celle-ci et à déclencher une vérification plus poussée. Ces outils permettent d'automatiser des méthodes manuelles afin d'examiner et de vérifier plus efficacement les tendances de consultation des DSE qui pourraient dénoter un accès illicite ou d'autres manquements à la conformité.

Protocoles d'anonymisation

L'anonymisation, nous le répétons, est l'un des outils de protection de la confidentialité les plus efficaces. Elle peut aider à se conformer aux principes de la réduction au minimum des données et à éviter les infractions à la confidentialité qui pourraient résulter du vol, de la perte ou d'une utilisation illicite des renseignements

personnels sur la santé. En même temps, elle peut faciliter l'utilisation de renseignements personnels sur la santé à d'importantes fins secondaires, par exemple la recherche en santé. L'anonymisation devient un outil encore plus puissant dans le contexte des DSE : ses techniques sont plus faciles à appliquer à des dossiers électroniques qu'à des dossiers papier, et il existe des logiciels qui permettent de retirer ou de supprimer automatiquement des identifiants directs d'un ensemble de données. Certaines méthodes d'anonymisation visent à réduire simultanément le risque de ré-identification et l'ampleur de la distorsion de la base de données d'origine, comme l'excellent outil d'augmentation de confidentialité mis au point par le Dr Khaled El Emam, qui peut être appliqué directement aux bases de données de renseignements personnels sur la santé[28]. Lorsqu'elle est faite de manière à réduire au minimum le risque de ré-identification tout en maintenant pour les données une qualité qui les rend aptes aux utilisations secondaires et qu'on procède à des recherches et à des rajustements constants pour remédier aux risques au fur et à mesure qu'ils se manifestent, l'anonymisation enchâsse une approche qui maximise les intérêts des dépositaires des données et des utilisateurs secondaires et, caractéristique primordiale, ceux des personnes à qui se rapportent les renseignements.

Gouvernance des renseignements contenus dans les dépôts de DSE

D'ores et déjà, les administrations s'attachent aux enjeux de gouvernance des données qui ont trait aux utilisations secondaires des renseignements conservés dans les DSE. Plusieurs d'entre elles ont nommé des dépositaires en chef ou des comités de fiducie des données qui sont chargés de passer en revue les demandes d'accès aux données et d'exercer une surveillance de la divulgation des données pour analyse. On s'attend à ce qu'il faille continuer à déployer des efforts pour établir les politiques et les pratiques exemplaires nécessaires à la régie des renseignements conservés dans les DSE, car plus la taille des entrepôts de données augmentera, plus leur valeur pour la recherche et les analyses augmentera aussi, et les pressions pour y accéder dans le cadre d'études fort diversifiées suivront le rythme.

Entrepôts de données

Plusieurs administrations ont mis sur pied des entrepôts de données qui recueillent, utilisent et divulguent des renseignements personnels sur la santé à des fins secondaires. Ces entrepôts sont aptes à offrir, dans le contexte des mégadonnées, une expertise sur les plus récentes façons de mettre en place des mesures de sécurité et de sauvegarde de la confidentialité, dont l'anonymisation. Les organismes qui chapeautent ces entrepôts sont eux-mêmes assujettis à des règles strictes qui les obligent à instaurer des pratiques et procédures visant à

28 L'outil d'anonymisation mis au point par le Dr El Emam établit une méthodologie pratique d'utilisation des techniques d'anonymisation et des instruments de mesure du risque de ré-identification permettant d'atteindre une qualité de données propice aux fins pour lesquelles les destine celui qui les reçoit et une protection du risque acceptable pour celui qui les divulgue. Voir CAVOUKIAN, A. et K. EL EMAM, « A Positive-Sum Paradigm in Action in the Health Sector », mars 2010. Accessible sur le web (en anglais seulement) à l'adresse suivante : http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf.

réduire à leur minimum les menaces à la sécurité et à la confidentialité associées aux renseignements qu'ils recueillent, utilisent et divulguent.

La LPRPS de l'Ontario, par exemple, établit des désignations particulières pour les personnes et organismes autorisés à recevoir sans consentement explicite des renseignements personnels sur la santé à des fins précises, par exemple l'analyse ou la recension de renseignements statistiques qui concernent la gestion du réseau de santé[29]. Toutefois, avant que des divulgations ne puissent être faites à ces organismes en Ontario, ils doivent être prescrits dans le règlement et avoir mis en place de solides pratiques et procédures visant à protéger et à maintenir la confidentialité des renseignements personnels sur la santé qui leur sont confiés. Ces pratiques et procédures doivent être officiellement approuvées et examinées tous les trois ans par le commissaire à l'information et à la protection de la vie privée de la province. Parmi les organismes en question, mentionnons l'Institut canadien d'information sur la santé, l'Institut de recherche en services de santé et Action Cancer Ontario.

Parmi les entrepôts de données situés à l'extérieur de l'Ontario, mentionnons Population Data BC (qui détient des données longitudinales anonymisées sur les quatre millions de résidents de la Colombie-Britannique), le Newfoundland and Labrador Centre for Health Information (un organisme d'État dont le mandat est d'intégrer et d'héberger des données émanant de toutes les composantes des systèmes de santé et de services communautaires de la province) et des instituts de recherche affiliés à des universités, comme l'unité de recherche sur la santé de la population de l'université Dalhousie, en Nouvelle-Écosse, le centre de recherche en politiques et en services de santé de l'université de la Colombie-Britannique, et le Manitoba Centre for Health Policy, affilié à la faculté de médecine de l'université du Manitoba. Les entrepôts de données qui obtiennent un statut particulier en vertu de la loi de la province sont autorisés à effectuer la manutention et la préparation de données brutes devant servir à des utilisations secondaires, en fonction de protocoles stricts et de mécanismes d'examen déontologiques visant à limiter aux seules personnes autorisées l'accès à des données identifiables et à veiller à ce que des pratiques adéquates de gestion des données aient été mises en place[30].

Formation sur la confidentialité et la sécurité

Une formation complète en confidentialité et sécurité fait aussi partie des principales composantes d'un cadre de protection de la confidentialité régissant les utilisations secondaires dans le contexte des DSE. Ce type de formation peut

29 Nommément « une personne prescrite qui dresse ou tient un registre de renseignements personnels sur la santé visant à faciliter ou à améliorer la fourniture de soins de santé ou concernant l'entreposage ou le don de parties du corps ou de substances corporelles » (LPRPS, alinéa 39(1) c); ou, dans le cas d'une entité prescrite, « un dépositaire de renseignements sur la santé (...) à des fins d'analyse ou de compilation de renseignements statistiques à l'égard de la gestion, de l'évaluation, de la surveillance ou de la planification de tout ou partie du système de santé ou de l'affectation de ressources à tout ou partie de celui-ci, y compris la prestation de services, si l'entité satisfait (à certaines autres) exigences (...) » (LPRPS par. 45 (1)).

30 WILLISON, *supra*, note 8, p. 22.

contribuer à réduire la fréquence des erreurs humaines et de la négligence qui sont souvent à l'origine des infractions à la confidentialité.

La formation peut aider à faire en sorte que les employés et agents soient conscients des obligations qui leur échoient en vertu de la loi ainsi que des politiques et procédures de confidentialité et de sécurité, pour ce qui touche la collecte, l'utilisation et la divulgation autorisées, ainsi que les mesures de sauvegarde qui doivent être mises en place pour protéger les renseignements personnels sur la santé dont on leur a confié la garde.

Dans le contexte des utilisations secondaires, la formation sur la confidentialité et la sécurité pose des problèmes supplémentaires. Les utilisateurs devront alors suivre une formation spécialisée et adaptée à leur rôle, qui reflète la nature particulière de cette activité et leur relation avec les dépositaires qui leur fournissent les données personnelles sur la santé dont ils ont besoin pour leur travail. Il y a aussi la question de savoir qui sera responsable d'assurer cette formation. Ces questions et d'autres encore peuvent être abordées dans les ententes sur la divulgation des données qui établissent les conditions rattachées aux utilisations secondaires prévues.

Politiques et procédures régissant les infractions à la confidentialité

Au Canada, nombre d'administration et d'organisations qui manipulent des renseignements personnels sur la santé ont déjà établi des politiques et procédures afin de régir l'identification, le signalement, la limitation, le rapport et l'enquête concernant les infractions à la confidentialité. Ces politiques et procédures peuvent aider à prévenir les infractions, à assurer une réaction prompte et coordonnée s'il s'en produit, à clarifier les rôles et responsabilités des employés et des agents dans de tels cas et à réduire au minimum les torts qui en résultent.

Les politiques et procédures devraient aussi s'attacher spécifiquement aux rôles et responsabilités des utilisateurs secondaires, qu'ils soient ou non des employés ou des agents du dépositaire des données, lorsque se produit une divulgation illicite des données. Par exemple, celles qui prévoient que la personne dont les données ont été divulguées doit en être informée pourraient ne pas être appropriées dans le cas où l'infraction est le fait d'un utilisateur secondaire sans lien direct avec elle. Dans ce cas, la politique pourrait exiger que les utilisateurs secondaires avisent le dépositaire des données, qui pourrait alors prendre les mesures voulues pour informer la personne en cause. Les ententes de divulgation des données qui régissent la relation entre l'utilisateur secondaire et le dépositaire des données devraient aussi clarifier la façon dont les politiques et procédures en cas de divulgation illicite s'appliquent aux utilisateurs secondaires.

Autres questions

Nous avons décrit plusieurs éléments d'un cadre de gouvernance régissant la protection de la confidentialité dans les utilisations secondaires. Ces éléments

sont soit déjà en place, soit accessibles sans avoir encore été adoptés à grande échelle, parce qu'il reste un certain nombre de problèmes à résoudre et d'éléments à examiner avant qu'ils soient à leur tour mis en place. Il y a aussi des questions sur la façon de concilier les différences, au chapitre des lois, politiques et procédures régissant les utilisations secondaires, entre les provinces et les territoires, entre les organismes d'une même province ou d'un même territoire, ou même entre les prestateurs de soins de santé proprement dits.

Si le *Recueil des notions communes* procure une certaine orientation, il demeure que des décisions critiques devront être prises sur ce à quoi ressemblera une structure globale de gouvernance de l'utilisation secondaire dans le contexte des DSE. Par exemple, il faut clarifier la question de la responsabilité. Qu'il soit question d'un dossier commun ou d'un dépôt de données de DSE, il importe d'établir l'identité du responsable du dossier et d'en déterminer le gardien, les responsabilités qui lui échoient à cet égard, l'obligation qu'il a d'aviser les intéressés de la possibilité que les renseignements aient été utilisés et les conditions dans lesquelles ceux-ci peuvent être divulgués pour une utilisation secondaire.

Il faut également déployer des efforts supplémentaires pour parvenir à rendre transparentes les utilisations secondaires actuelles et futures dans le contexte des DSE. L'approbation et l'accréditation des dépôts de données, par exemple, peuvent non seulement permettre d'en documenter systématiquement l'existence, mais aussi d'uniformiser les critères régissant leurs créateurs et gestionnaires et les conditions auxquelles ils doivent satisfaire pour agir à ce titre[31]. En outre, une structure de rapport pourrait être créée, suivant laquelle le public et les utilisateurs secondaires possibles pourraient être avisés de l'existence de dépôts de données, notamment par l'affichage sur le web d'une liste de ces dépôts, ainsi que de toutes les utilisations et les divulgations qui seraient faites. Par exemple, un registre peut être créé pour porter à la connaissance du public, de façon continue, la création d'études de recherche qui ont recours aux renseignements contenus dans les DSE, la nature de leurs travaux et leurs conclusions[32].

Un autre aspect de la question mérite attention : les formes que peut prendre le consentement à l'utilisation secondaire des renseignements contenus dans le contexte des DSE. D'aucuns ont proposé de nouvelles approches à cet égard, étant donné que les modèles de consentement conventionnels préconisant soit un consentement tous azimuts aux activités de chaque projet, soit une exemption pure et simple de consentement conviennent bien mal à l'éventail d'utilisations auxquelles pourraient se prêter un jour les DSE. Les stratégies les plus variées ont été proposées, depuis l'élimination radicale du consentement jusqu'à un consentement d'office à toute divulgation et à toute utilisation possible et imaginable, en passant par un élargissement des exemptions au consentement et par un consentement réputé s'appliquer rétroactivement[33]. Autre proposition : un modèle de consentement à niveaux multiples, qui comporterait diverses options de

31 *Ibid.*, p. 23.

32 Kosseim, *supra*, note 8, p. 24.

33 *Ibid.*, pp. 20-43.

consentement implicites à divers types d'utilisations secondaires selon la nature de l'utilisation, les avantages que pourrait en retirer la société, les risques pour la personne, le potentiel de commercialisation et d'autres facteurs[34].

Si on n'a toujours pas trouvé de modèle pratique et fonctionnel, le débat sur la question est critique parce que l'avenir des utilisations secondaires va en dépendre. En outre, même si l'approche stratégique adoptée au bout du compte est axée sur le consentement, une question pratique demeure : comment inscrira-t-on dans le DSE le consentement du patient et ses préférences quant aux utilisations secondaires, y compris celles qui peuvent ne pas avoir encore été définies? Dans l'un de ses projets sur la gestion du consentement, Inforoute Santé du Canada prévoit que le DSE pourra servir à consigner le consentement pour des recherches ultérieures et en a donc fait une exigence administrative et architecturale pour toute solution de gestion du consentement[35]. Autre solution possible : utiliser un portail ou d'autres moyens électroniques par lesquels les patients pourraient documenter et inscrire leurs préférences quant aux utilisations secondaires et être informés des utilisations, le cas échéant. De plus, des technologies de gestion numérique des droits pourraient être mises en application pour contrôler la durée du consentement aux utilisations secondaires et circonscrire les paramètres de la divulgation et des utilisations. Il existe un modèle d'outil qui permettra un jour d'obtenir une maîtrise totale des renseignements personnels : le modèle « SmartData », créé à l'Université de Toronto par le Dr Tomko[36].

D'aucuns allèguent aussi qu'il faudrait, dans le contexte d'un nouveau DSE, revoir en profondeur certains concepts, par exemple établir de nouvelles distinctions entre les utilisations primaire et secondaire, et entre certains types d'utilisation secondaire, comme la recherche et l'amélioration de la qualité. Certains auteurs proposent que la recherche sur la santé, qui est typiquement considérée comme une utilisation secondaire, soit désormais assimilée à une utilisation primaire en raison de la relation entre la santé des personnes et des populations, d'une part, et les soins de santé publics et la recherche financée par le secteur public, d'autre part. Ils soulignent que les progrès réalisés en informatique, en génomique et dans d'autres domaines ont contribué aux progrès rapides des soins de santé, de sorte qu'il est plus probable que jamais qu'une personne puisse voir de son vivant les avantages directs, pour elle-même et pour sa famille, d'une participation à la recherche[37]. De même, la distinction entre la recherche et d'autres utilisations secondaires comme la planification des systèmes et l'amélioration de la qualité, qui

34 CAULFIELD et coll. et SINGLETON et coll., cités dans Willison, *supra*, note 7, pp. 9, 18-21; Kosseim, *supra*, note 8, p. 45.

35 Inforoute Santé du Canada, *Business and Architecture Considerations for Interoperable Solutions, a discussion document* (inédit).

36 Le programme SmartData suppose l'utilisation d'agents virtuels intégrés dans les systèmes informatiques, qui joueront en ligne le rôle de délégués de la personne en entreposant de façon sûre ses renseignements personnels et en les divulguant intelligemment, en fonction des critères retenus par elle. SmartData permettrait la divulgation des renseignements d'après le contexte des demandes, selon les autorisations données par la personne concernée par les données. Voir TOMKO, George J. et coll., « SmartData: Make the data "think" for itself » in *Identity in the Information Society*, vol. 3 no 2, 2010, p. 343.Accessible sur le web (en anglais seulement) à l'adresse suivante : http://www.springerlink.com/content/1883257206825632/fulltext.pdf.

37 Kosseim, *supra*, note 9, pp. 31-35; Willison, *supra*, note 8, pp. 15-17.

n'exigent pas de consentement et ne sont pas sujettes à des examens déontologiques aussi rigoureux, est remise en question[38]. Certains analystes ont fait remarquer que les modèles actuels d'autorisation de la recherche demeurent largement axés sur des études de recherche distinctes, dont les objectifs définis peuvent être reliés à la collecte de données précises, et ne s'appliquent donc pas d'emblée aux données contenues dans les DSE, lesquelles peuvent servir de plateformes de recherche pour des utilisations fort diversifiées[39]. On a aussi allégué que les variations des règles de la recherche[40] et des décisions des comités d'éthique en recherche selon l'endroit au pays[41] généraient une incohérence et une incertitude qui peuvent freiner l'adoption de systèmes de DSE interopérables pour la recherche à laquelle participent plusieurs provinces, territoires ou administrations.

À mesure que les projets de recherche univalents mènent à la création de dépôts de données qui serviront de plateforme à une diversité d'utilisations secondaires futures des DSE, certains ont évoqué la possibilité d'éliminer les frontières entre les divers types d'utilisations secondaires et suggèrent de ce fait d'appliquer une approche commune et proportionnée de l'examen éthique de toutes les utilisations secondaires en fonction du risque auxquels sont exposées les personnes dont les renseignements sont sujets aux utilisations en question[42].

La solution à ces questions et à bien d'autres exigera un apport constant de la part de toutes les parties prenantes, dont les législateurs, les décideurs, les prestateurs de soins de santé, les utilisateurs secondaires, les concepteurs de systèmes et, surtout, le public, dans le cadre d'une conversation pancanadienne sur l'évolution idéale d'une structure régissant les utilisations secondaires des DSE. Il faudra aussi adopter la PIVP, dont la souplesse permettra de réagir aux problèmes à mesure qu'ils se présentent et de protéger la confidentialité des renseignements personnels tout en en facilitant une utilisation secondaire appropriée.

Conclusions

Nous avons vu en quoi les caractéristiques intrinsèques des DSE qui en font un outil précieux de la modernisation des systèmes d'information dans le secteur de la santé compliquent le maintien de la confidentialité des renseignements personnels sur la santé qu'ils contiennent. Malgré ces difficultés, nous reconnaissons à quel point il est important de mettre à profit la puissance des systèmes de DSE pour permettre une utilisation plus rapide, plus sûre et plus efficace des renseignements pour les utilisations primaires et secondaires.

38 Willison, *supra*, note 8, pp. 7-8.

39 WILLISON, D., « Data Protection and the Promotion of Health Research: If the Laws Are Not the Problem, Then What Is? » *in Healthcare Policy* 39, vol. 2 nº 3, 2007, pp. 40-41.

40 Kosseim, *supra*, note 9, p. 36.

41 Willison, *supra*, note 8, pp. 9, 24.

42 *Ibid.*, p. 16.

Le projet de longue haleine visant le déploiement de DSE communs et interopérables est bien amorcé. Les provinces et territoires canadiens en sont à des étapes diverses de la mise en service des composantes de leurs systèmes de DSE. L'adoption de plus en plus répandue des technologies informatiques et la sensibilisation croissante aux avantages de l'utilisation des renseignements électroniques pour les soins de santé et à d'autres fins nous permettent de croire que le nombre d'entrepôts de données augmentera, au rythme de l'intégration des données et de la hausse du nombre de demandes d'accès aux renseignements électroniques et de leurs utilisations possibles.

Le soutien accordé à l'utilisation secondaire dans le contexte des DSE interopérables sera tributaire du développement constant d'un cadre de gouvernance qui appuie des utilisations appropriées, coordonnées et soucieuses de la confidentialité des renseignements électroniques sur la santé, tant au sein de chaque administration que dans leurs échanges. S'il est vrai que, comme nous l'avons dit, nombre d'éléments de cette structure sont déjà en place, il demeure qu'il faut poursuivre partout au pays la discussion sur l'établissement d'un cadre clair et cohérent qui faciliterait le maintien des utilisations secondaires. Cette discussion doit reposer sur une caractéristique essentielle et incontournable : seuls des renseignements anonymisés doivent être utilisés ou divulgués à des fins secondaires et, lorsqu'ils ne suffisent pas, il faut prévoir au préalable des garanties supplémentaires de protection de la confidentialité. Si l'on veut que tout ce qui doit raisonnablement être fait soit bel et bien fait, il faut en discuter le plus rapidement possible. Ce n'est qu'à ce prix qu'on pourra maintenir des utilisations secondaires qui respectent vraiment la confidentialité – et arriver à une situation où tout le monde gagne.

Commissaire à l'information et à la protection de la vie privée de l'Ontario
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8
Site web: www.ipc.on.ca
Protection intégrée de la vie privée : www.privacybydesign.ca

Inforoute Santé du Canada
1000, rue Sherbrooke Ouest
Bureau 1200
Montréal (Québec) H3A 3G4
Site Web : www.inforway-inforoute.ca

L'information figurant dans les présentes peut être modifiée sans préavis. *Inforoute* et le CIPVP ne peuvent être tenus responsables d'omissions ou d'erreurs techniques ou typographiques contenues aux présentes.

2 Mars 2012