

Commissariat à la protection de la vie privée

Ici, maintenant et après : protection de la vie privée et dossiers de santé électroniques

Troisième conférence annuelle sur les dossiers de santé électroniques et les systèmes d'information

Le 28 novembre 2006
Toronto (Ontario)

Allocution prononcée par Patricia Kosseim
Avocate générale, Commissariat à la protection de la vie privée du Canada

Introduction

Au nom du Commissariat à la protection de la vie privée du Canada, je vous remercie de m'avoir invitée à prendre la parole ici aujourd'hui.

L'autre jour, je suis tombée par hasard sur une citation du poète et essayiste John Perry Barlow, qui disait ceci :

« Compter sur le gouvernement pour protéger la vie privée, c'est comme demander à un voyeur d'installer vos stores. »

La citation de Barlow reflète certaines de nos peurs les plus profondes que des organismes publics utilisent nos renseignements personnels à mauvais escient. Pour nous, qui avons à cœur de veiller à ce que la vie privée soit protégée, cela renforce notre message, soit l'importance de conserver la confiance du public.

Le Commissariat suit de près l'élaboration de systèmes interexploitables de dossiers de santé électroniques (DSE) au Canada. Si de tels systèmes sont mis au point, nous devons engager **dès maintenant** un débat public transparent sur les répercussions qu'aurait l'utilisation actuelle et future de ces systèmes sur la protection de la vie privée. Ce n'est que par une discussion ouverte et franche que le public fera confiance à l'équilibre de poids et de contrepoids qui a été – et qui doit encore être – intégré aux systèmes de dossiers de santé électroniques.

Alan Westin, l'un des grands ténors de la protection de la vie privée aux États-Unis, a déclaré ceci au sujet de l'adoption par son pays des dossiers de santé électroniques :

« Je suis convaincu que c'est essentiellement la façon dont le public perçoit les risques à l'égard de la vie privée et la prévention

des abus dans tout système de dossiers de santé électroniques qui assurera le succès du programme – ou qui constituera un facteur déterminant de son échec. »

Une telle affirmation n'en est pas moins vraie ici au Canada, plus particulièrement au moment où les dossiers de santé électroniques sont utilisés à d'autres fins que les soins directs prodigués aux patients – comme la recherche en santé, l'emploi et l'assurance. D'autres usages des DSE – usages que nous aurions jugés « futuristes » il y a à peine quelques années – nous sont déjà imposés. Enfin, il y a aussi les utilisations illicites appréhendées des DSE, lesquelles constituent désormais une véritable et puissante menace dans un monde où le risque de vol d'identité s'avère de plus en plus élevé. Permettez-moi de prendre les prochaines minutes pour aborder quelques-uns des « autres » usages des DSE.

Recherche en santé

Jusqu'à maintenant, les DSE nous ont été présentés comme une innovation merveilleuse qui améliorera la qualité, la prestation et l'efficacité des soins directs prodigués aux patients. Or, nous savons également que le caractère interexploitable des dossiers donnera probablement lieu à une accumulation de données, lesquelles serviront à créer ou à alimenter des plates-formes de recherche nationales en matière de santé.

Bien que l'élaboration de telles plates-formes soit certainement un objectif louable – objectif qui, le croyons-nous et l'espérons-nous, permettra d'améliorer les soins accordés aux patients –, il ne faut pas oublier que du point de vue des patients, l'utilisation de leurs renseignements médicaux personnels à des fins de recherche soulève des considérations tout à fait différentes de celles concernant l'utilisation de la même information pour leur bénéfice direct et immédiat. Il nous faut faire preuve de la plus grande transparence auprès des Canadiennes et des Canadiens, de sorte qu'ils puissent également intégrer ces autres considérations aux conditions qu'ils acceptent, à titre de patients, dans le cadre de ce nouveau contrat social concernant les DSE.

On doit expliquer clairement aux Canadiennes et aux Canadiens que leurs données comprises dans les DSE pourraient éventuellement être utilisées à des fins de recherche. De fait, cela oblige la reconnaissance publique de la réalité suivante :

- l'accès aux données des DSE à des fins de recherche en santé pourrait exiger l'accès à des données identifiables au sujet de personnes;
- la recherche en santé pourrait être financée par les deniers publics, ou en totalité ou en partie par des sources privées animées par la recherche de profit;
- il ne sera pas toujours possible d'obtenir le consentement éclairé et individuel des patients à chaque étape du processus;
- le sujet de la recherche effectuée peut être considéré par certaines personnes comme immoral;
- la profession de chercheur n'est pas aussi réglementée que celle des pourvoyeurs de soins de santé;
- bien que des comités d'éthique en matière de recherche puissent donner

leur autorisation, la gouvernance de ces comités au Canada comporte des enjeux majeurs qui devront être abordés.

Je suis certaine que vous conviendrez qu'il s'agit là de considérations éminemment importantes qui doivent être discutées publiquement dès aujourd'hui, et non de considérations dont l'examen doit être reporté à plus tard. Bien que de telles considérations **ne doivent aucunement** freiner la recherche dans le domaine de la santé, les Canadiennes et les Canadiens ont le droit d'être pleinement informés des conditions qu'ils acceptent lorsqu'ils participent à l'utilisation de nouveaux systèmes de DSE. Nous ne pouvons pas attendre que ces systèmes soient pleinement opérationnels et retarder les applications de la recherche pour ensuite invoquer le caractère peu pratique de la chose pour justifier de n'avoir pas fait appel au consentement des Canadiennes et des Canadiens.

Emploi et assurance

Au moment où les systèmes interexploitables de DSE remplacent les amoncellements multiples de dossiers papier chez divers pourvoyeurs de services de santé, les pressions qu'exercent les assureurs et les employeurs pour obtenir un accès facile et à guichet unique à de plus en plus de données augmenteront considérablement.

Bien que le consentement exprès des personnes sera manifestement requis pour permettre à des tiers d'avoir accès à des données des DSE, l'enjeu (même dans un monde où il n'y a que des dossiers papier) demeure essentiellement la validité de ce consentement – à savoir s'il s'agit d'un consentement éclairé et volontaire. Dans l'état actuel des choses, pour accéder à des dossiers médicaux papier, on obtient en général le consentement en enfouissant des clauses de consentement obscures et au libellé fort élastique dans des contrats complexes et longs. Qui plus est, on exige souvent le consentement général comme condition nécessaire pour qu'une personne obtienne une assurance, voire un emploi.

Les DSE ne viendront qu'amplifier ces problèmes en offrant plus facilement à des tiers un accès général à davantage de données biographiques, médicales et génétiques ainsi qu'à des renseignements sur le mode de vie – beaucoup plus de données en fait que ce dont on aurait normalement besoin sur une personne, et beaucoup plus que ce que la plupart des personnes accepteraient de donner si elles avaient vraiment le choix.

Récemment, le Québec a abordé cet enjeu en modifiant sa loi sur la santé et les services sociaux pour interdire aux assureurs ou aux employeurs de demander l'accès au DSE d'une personne – même avec le prétendu consentement de cette dernière. Reste à voir comment les autres provinces et territoires réagiront aux pressions de plus en plus grandes exercées par les employeurs et les assureurs pour avoir un accès général aux DSE à des fins autres que la prestation de soins de santé. En ce qui concerne la **LPRPDÉ**, je peux vous assurer que nous allons surveiller la situation d'un œil très attentif.

Utilisations « futuristes »

Il y a aussi d'autres utilisations « futuristes » des DSE qui, il y a à peine quelques

années, auraient fait partie de la science-fiction, mais qui, aujourd'hui, sont devenues réalité.

Vous avez probablement déjà entendu beaucoup parler d'une société de la Floride, VeriChip Corporation. L'entreprise – qui, soit dit en passant, a des bureaux à Vancouver et à Ottawa – se targue d'avoir conçu et breveté une micropuce d'identification par radiofréquence pouvant être implantée chez l'humain et qui est approuvée par la FDA. Cette micropuce – qui est à peu près de la taille d'un grain de riz – peut être implantée sous la peau des patients. Elle contient un numéro d'identité unique qui peut être lu par le personnel des services d'urgence à l'aide d'un scanner manuel afin d'établir un lien immédiat entre un patient inconscient ou léthargique et son dossier de santé inscrit dans une base de données supposément sûre. Le produit prétend offrir un lien vital salutaire entre les patients et le personnel médical. La société a annoncé récemment que 1 100 médecins et 260 hôpitaux aux États-Unis se sont inscrits pour apprendre comment implanter et balayer les puces électroniques. Cependant, comme le rappelle souvent Ian Kerr, professeur à l'Université d'Ottawa, la lisibilité de ces puces d'identification suscite des problèmes graves à l'égard de la protection de la vie privée, mais aussi de la sécurité, et elle a d'importantes répercussions sur les politiques visant à réglementer de telles micropuces au Canada qui ne correspondent pas tout à fait à la définition d'un dispositif médical en vertu de la **Loi sur les aliments et drogues** du Canada.

De l'autre côté de l'Atlantique, un projet de télémédecine que l'on appelle DICOEMS, financé par l'Union européenne, a également pour but de trouver des façons d'établir un lien entre les patients en situation d'urgence et leur dossier de santé électronique, en utilisant notamment leur ADN. Les responsables du projet auraient, dit-on, tenté de créer un dispositif qui pourrait analyser l'ADN d'un patient hospitalisé et l'apparier immédiatement à un fichier contenant son dossier médical. Cependant, le projet n'a pas été un succès parce qu'il n'existe actuellement aucun cadre juridique dans l'Union européenne qui appuie la création d'une base de données complète d'ADN qui proviennent du grand public.

Ce que ces deux exemples de développement illustrent clairement, c'est que, en tant que société, nous tentons de déployer tous les efforts nécessaires pour suivre les nouvelles technologies – ou pour adapter des technologies existantes à des fins nouvelles. Pour parvenir à élaborer une politique gouvernementale régissant l'utilisation appropriée de ces technologies, il nous faut, à tout le moins, un débat public plus large, plus inclusif et plus transparent sur les questions de protection de la vie privée qui sont en jeu.

Utilisations illicites

Parallèlement à ces utilisations délibérées et intentionnelles des DSE, d'autres utilisations non prévues, non intentionnelles et non désirées se cachent sur fond de vols d'identité de plus en plus fréquents.

Pour vous donner un exemple, permettez-moi de vous faire part d'un reportage publié dans l'édition de septembre dernier du Times de Los Angeles intitulé « ID Theft Infects Medical Records » (Les vols d'identité infectent les dossiers médicaux). L'auteur de l'article décrit comment la vie privée d'une personne peut être compromise au point où non seulement sa sécurité médicale, mais aussi sa

vie privée, s'en trouvent affectées.

Au début de l'année, l'agence locale de services sociaux a communiqué avec une mère de quatre enfants de Salt Lake City pour lui dire que son poupon hospitalisé avait subi des tests démontrant qu'il avait été en contact avec des drogues illicites et que les services sociaux allaient venir chercher tous ses enfants. Or, la mère n'avait donné naissance à aucun enfant depuis deux ans et n'avait pas d'enfant non plus à l'hôpital. Cette femme était dans tous ses états. Elle n'est pas parvenue à persuader les services sociaux qu'une erreur avait été commise. Ce n'est qu'après que le travailleur social eut bombardé de questions son enfant de sept ans pour savoir si sa mère avait été à l'hôpital dernièrement que l'agence des services sociaux est revenue sur sa décision.

Or, il s'est avéré que quelqu'un avait volé le permis de conduire de cette femme quelques mois auparavant dans la voiture de son mari. L'usurpatrice qui l'avait volé a utilisé le permis de conduire pour s'identifier lorsqu'elle est entrée à l'hôpital afin d'accoucher. Comme cette femme était déjà recherchée pour d'autres accusations de vol d'identité, elle ne voulait pas utiliser sa propre carte de crainte d'être arrêtée.

Lorsque la mère de quatre enfants a par la suite contracté une infection rénale, elle a pris les moyens qu'elle estimait être sûrs : pour éviter toute autre confusion, elle a, à dessein, choisi un établissement dans lequel ni elle ni l'usurpatrice ne pouvaient avoir été hospitalisées dans le passé. Cependant, certains dossiers avaient été transmis électroniquement entre les hôpitaux. Ainsi, le groupe sanguin inscrit à son dossier était celui de l'usurpatrice. Heureusement, les employés de l'hôpital ont vérifié et repéré le problème; s'ils ne l'avaient pas fait, le résultat aurait pu être désastreux. Mais ce n'est pas tout : il s'est avéré que le nom de la personne-ressource en cas d'urgence et le numéro de dossier étaient également erronés.

Cette histoire montre les dangers qui peuvent survenir lorsque des renseignements personnels sur une personne sont mal utilisés dans un système interexploitable de DSE. Tandis que les DSE offrent certainement la possibilité d'une plus grande sécurité, facilitent les vérifications et les mesures d'authentification, ils réduisent également les démarches qu'on devrait faire pour s'assurer de leur exactitude, ce qui, dans le cas d'une identité volée, pourrait s'avérer fatal.

À mesure que nous continuons de concevoir des systèmes interexploitables de DSE, nous ne pouvons pas le faire en vase clos. La réalité de la fraude et du vol d'identité doit être prise en compte afin de réduire les risques d'erreurs à vous faire dresser les cheveux sur la tête. L'impact potentiel sur la confiance du public pourrait être énorme.

Dans un rapport récent intitulé ***Building Privacy by Design in Health Data Systems***, Alan Westin s'intéresse à plusieurs facteurs ayant eu une incidence considérable sur la mise en œuvre des DSE aux États-Unis, notamment la « multiplication en 2004-2005 d'incidents impliquant la communication et la compromission de dossiers médicaux personnels par des pourvoyeurs de services de santé et ce, dans un contexte national où l'on assiste à une augmentation de fraudes et de vols d'identité » [Traduction]. Selon Alan Westin, c'est pour cette raison que les sondages de 2005 indiquent que la population répond tout autant par l'affirmative que par la négative quand on lui demande si les avantages d'une informatisation et d'un réseautage plus poussés dans le

domaine des soins de santé excèdent les risques potentiels d'atteinte à la vie privée.

Les DSE et le Commissariat

Bien que les DSE interexploitables offrent des avantages énormes et la possibilité d'une qualité, d'une utilisation et d'une efficacité supérieures du système de soins de santé au Canada, il n'en demeure pas moins qu'il y a d'importantes répercussions sur la vie privée qu'il faudra prendre en compte à mesure que les DSE seront utilisés et déployés à des fins autres que les soins directs prodigués aux patients.

Afin de faire progresser le débat sur ces enjeux, le Commissariat finance d'importants projets de recherche sur divers aspects des DSE.

- Le premier vise à financer le Centre de bioéthique à l'Institut de recherches cliniques de Montréal, un projet qui examine les défis que les utilisations secondaires des DSE posent à l'égard de la vie privée.
- Le Commissariat soutient un projet de recherche de l'Université Memorial de Terre-Neuve dont le sujet est l'interaction – dans le secteur des soins de santé - entre les options offertes par les technologies de l'information et les politiques des gouvernements émises conséquemment.
- Le troisième projet est mené au Children's Hospital of Eastern Ontario Research Institute pour concevoir des lignes directrices pancanadiennes sur la dépersonnalisation des renseignements personnels sur la santé à partir d'une étude empirique sur les divers risques de nouvelle personnalisation qui existent actuellement au Canada.

Conclusion

Il ne fait aucun doute que les systèmes de DSE sont la voie de l'avenir; les possibilités qu'ils offrent d'améliorer les soins de santé sont énormes. Cependant, on ne peut pas se permettre de nier la nécessité de préserver la collaboration et la confiance des Canadiennes et des Canadiens en même temps que se développent les systèmes de DSE et que ceux-ci sont déployés à des fins autres que la prestation de soins directs aux patients.

À mesure que le Canada met de l'avant ces systèmes de DSE, nous risquons de perdre la confiance des Canadiennes et des Canadiens si nous ne nous engageons pas dans un débat ouvert et honnête sur les développements éventuels de ces systèmes et l'utilisation probable qui en sera faite dans le futur.

Si des systèmes interexploitables de DSE sont implantés et développés au cours des prochaines années, il nous faudra compter sur la confiance des Canadiennes et des Canadiens. Actuellement, nous semblons avoir une certaine crédibilité à l'égard du public. Si nous pouvions avoir un véritable débat public sur l'utilisation potentielle des DSE à d'autres fins et ce, de façon franche, inclusive et transparente, et si nous intégrions actuellement aux systèmes les protections nécessaires pour respecter le droit des personnes à la vie privée, nous aurions une bonne chance de maintenir cette confiance et de l'utiliser au maximum pour exploiter le plein potentiel des DSE.

Merci.

Date de diffusion : 2007-01-19
Date de modification : 2007-01-19 ▲

[Avis importants](#)