CONSEILS MARSH :

ATTÉNUATION DES CYBERRISQUES DES ÉTABLISSEMENTS DE SOIN DE SANTÉ

Il est manifestement admis que, de manière fondamentale et inhérente, les relations avec les fournisseurs de soins de santé reposent sur la confiance, de sorte que les professionnels ont la responsabilité de protéger leurs clients et patients. La notion de respect de la vie privée des patients est aussi vieille que la profession de médecin et elle est expressément visée par le serment d'Hippocrate.

Bien que les erreurs de médication et les événements ou les résultats indésirables mettent régulièrement cette relation à l'épreuve, la nouvelle menace que constituent les atteintes à la confidentialité et aux données personnelles se révèle tout aussi dangereuse.

CONTEXTE

Le passage aux dossiers de santé électroniques a soulevé de nombreux problèmes et a fait apparaître un type de risque inédit : les atteintes à la confidentialité et aux données personnelles. La cybersanté était censée améliorer le partage de données et l'accès à celles-ci, faire baisser les coûts grâce à la collaboration, et réduire les services en double. Elle a finalement entraîné une perte de connaissances et des difficultés d'identification des données en ce qui concerne les stratégies d'atténuation, la prévention et la mise en œuvre efficace de mesures.

Aux États-Unis, les partisans de la cybersanté soutenaient la nécessité de passer aux dossiers de santé électroniques afin d'améliorer la qualité et la rentabilité des soins. Les organismes de soins de santé n'étaient toutefois pas préparés à la possibilité du matraquage des atteintes et infractions à la confidentialité.

Au Canada, deux lois fédérales régissent actuellement la sécurité des données personnelles : la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Loi sur la protection des renseignements personnels se rapporte au droit qu'ont les personnes « d'avoir accès aux renseignements personnels les concernant qui sont détenus par le gouvernement du Canada et de demander que des corrections y soient apportées, et énonce la manière dont le gouvernement peut recueillir, utiliser et communiquer ces renseignements personnels dans le cadre de la prestation de services[1] ». Il est important de noter que cette loi s'applique seulement aux institutions du gouvernement fédéral. Le Commissariat à la protection de la vie privée du Canada surveille le respect de cette loi.

1 Gouvernement du Canada, consulté le 8 avril 2015, https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_f.asp

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES (LPRPDE)

Cette loi « définit les règles applicables à la collecte, à l'utilisation et à la communication des renseignements personnels par les organismes du secteur privé dans le cadre d'activités commerciales au Canada[2] » (et elle ne s'applique pas aux organismes sans but lucratif et aux organismes de charité). La loi s'applique plus particulièrement aux :

- organismes du secteur privé qui exercent des activités dans les provinces et territoires suivants : Île-du-Prince-Édouard, Manitoba, Nouveau-Brunswick, Nouvelle-Écosse, Nunavut, Ontario, Saskatchewan, Terre-Neuve-et-Labrador, Territoires du Nord-Ouest ou Yukon;
- employés d'organismes du secteur privé qui exercent des activités au Canada, s'il y a transfert interprovincial ou international des renseignements personnels recueillis, utilisés ou communiqués;
- organismes sous réglementation fédérale, par exemple les banques, les transporteurs aériens, y compris en ce qui a trait au traitement des renseignements sur la santé et concernant les employés.

Chaque province ou territoire a promulgué une loi régissant la protection des renseignements personnels dans le secteur public. Le texte de ces lois peut être consulté en ligne.

TENDANCES DES ATTEINTES AUX DONNÉES PERSONNELLES DANS LES SOINS DE SANTÉ

Selon Khalid El Emam, de la chaire de recherche du Canada en soins de santé de l'Université d'Ottawa, deux grandes tendances se dessinent actuellement en ce qui concerne les données des soins de santé : la numérisation de l'information des soins de santé (y compris les dossiers médicaux électroniques et les dossiers de santé médicaux) et la monétisation de ces données. Celle-ci entraîne des risques importants – aux patients et au fournisseur ou à l'organisme de soins de santé. En raison de leur valeur pécuniaire, ces données sont plus utiles au domaine commercial qu'aux criminels.

Pour El Emam, le détournement de l'utilisation initiale des données pour des usages secondaires (tels que le développement de logiciels, la recherche et l'exploitation théorique) est à l'origine de leur valeur commerciale, alors que leur valeur criminelle dérive souvent d'activités illégales (notamment de la fraude, d'allégations fallacieuses et de l'acquisition de prescriptions de substances contrôlées à des fins de recel[3]).

IMPLICATIONS DES ATTEINTES AUX DONNÉES PERSONNELLES

Selon le Journal de l'Association médicale canadienne qui partage l'opinion d'El Emam, « les atteintes à la vie privée sur les appareils mobiles sont problématiques au Canada[4] ». En conséquence de ces menaces potentielles, les Canadiens hésitent à dévoiler leurs renseignements personnels aux fournisseurs de soins de santé. Pour les besoins du sondage en ligne intitulé « Canada: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcome », 1 002 Canadiens ont été interrogés et « 43,2 % [d'entre eux] ont tu ou tairaient des renseignements à leurs fournisseurs de soins de santé en raison de problèmes de confidentialité, et 42,9 % [d'entre eux] préféreraient trouver des soins à l'extérieur de leur communauté[5] ».

Les menaces et atteintes à la confidentialité courantes sont les suivantes :

- La collecte de données.
- L'utilisation et la divulgation de données.
- L'accès non autorisé.
- L'usage secondaire.
- Les erreurs.

---

2 Ibid.

3 Roger Collier, publié en premier lieu le 6 février 2012, doi : 10.1503/cmaj.109-4116 CMAJ 6 mars 2012 vol. 184 no 4 E215-E216

4 Ibid.

5 Ibid.

- La conception du dossier de santé électronique.
- Le manque de normes[6].

Selon Parks et autres (2011), diverses stratégies techniques d'atténuation ont été élaborées afin de contrer les atteintes à la confidentialité et les problèmes de sécurité potentiels. Il faut également noter que ces stratégies d'atténuation sont conservatrices par nature. On a également essayé de créer et d'élaborer des contre-mesures aux menaces contre la sécurité ci-dessus, par exemple :

- Mesures techniques (par ex. le chiffrement, la dépersonnalisation, l'anonymisation, les audits d'exploration des données, la corruption des données, la suppression à distance des données en cas de perte ou de vol d'appareil[7]).
- Accès (par ex. proposer un accès sans stockage sur les appareils mobiles, stockage limité aux données dépersonnalisées, permettre aux pistes d'audit de suivre l'information désignée sur la santé sur des appareils mobiles, codes d'accès[8]).
- Mise au point de politiques (par ex. relatives à la production de rapports, aux atteintes à la confidentialité).
- Formation et sensibilisation.
- Adoption d'une nouvelle culture (par ex. mise au point d'une culture axée sur la prise de conscience de l'existence de risques, afin d'obtenir une grande responsabilisation).

FACTEURS HUMAINS

La divulgation de renseignements personnels médicaux est le deuxième type d'atteintes aux données courantes[9]. Comme les exigences réglementaires et législatives façonnent toujours l'industrie, de nouvelles exigences techniques et logicielles ou en matière d'adoption de politiques et de mise en conformité sont constamment imposées et mises en œuvre. Mais qu'en est-il du facteur humain?

La transmission de savoirs, la sensibilisation et la formation doivent également être des éléments clés de la stratégie d'atténuation des organismes. En adoptant une culture axée sur la sensibilisation aux risques, les organismes peuvent expliquer à tous leurs membres qu'ils sont responsables de garantir la sécurité et la protection des renseignements personnels de santé. La haute direction a la responsabilité de faire avancer cette idée et de s'assurer que tous les intéressés y adhèrent.

Voici des exemples de stratégies d'atténuation axées sur le facteur humain :

- Gestion du changement.
- Adoption d'une nouvelle culture.
- Sensibilisation.
- Formation.
- Changement de comportement.

AVANTAGES DE L'INVESTISSEMENT

La plupart des organismes reconnaissent que leurs dépenses en capital importantes imposent d'assurer la sécurité et l'intégrité des renseignements de soins de santé. L'analyse coûts-avantages indique toutefois clairement les nombreux avantages d'un tel investissement.

RISQUES LIÉS À LA RÉPUTATION

En qualité de gardien des renseignements de soins de santé, les organismes ont l'obligation fiduciaire de protéger leurs patients et membres. À ce titre, cette obligation impose entre autres choses la protection des renseignements sur la santé personnelle. Les atteintes aux données entraînent des dommages dévastateurs et parfois irréversibles à l'actif le plus important d'un organisme : sa réputation. En raison des nouveaux modèles de financement, ce qui précède peut-être à l'origine d'une baisse d'activité et d'une chute du chiffre d'affaires de l'organisme.

---

6 Parks, Rachida; Chu, Chao-Hsien et Xu, Heng, Healthcare Information Privacy Research: Iusses, Gaps and What Next? (2011).

7 Ibid.

8 Parks, Rachida; Chu, Chao-Hsien et Xu, Heng, Healthcare Information Privacy Research: Iusses, Gaps and What Next? (2011). 9 Comité consultatif canadien sur les soins infirmiers

9 Hasan, R., and Yurcik, W. A Statistical Analysis of Disclosed Storage Security Breaches, Proceedings of the Second ACM Workshop on Storage Security and Survivability (StorageSS), ACM, Alexandria, Virginia, À.-U., 2006, p. 1-8.

MARSH

RISQUES FINANCIERS

Les atteintes aux données ont automatiquement des conséquences sur les finances des organismes de soins de santé. Le total des pertes économiques annuelles liées aux atteintes aux données dans les hôpitaux américains s'élève à 6 G$[10]. Les coûts des atteintes elles-mêmes comprennent les dépenses pour les enquêtes et les frais juridiques, le processus de notification, les exigences en ressources humaines, la restauration des données et les litiges potentiels. Selon El Emam, le coût moyen d'une atteinte est environ de 200 $ à 300 $ par dossier, ce qui peut se traduire par des millions de dollars pour un organisme et ainsi limiter ses ressources ou découler sur une réduction des offres de programmes ou de soins destinés aux patients. L'atténuation et le transfert des risques sont des solutions alternatives adéquates et doivent faire partie de la stratégie de réduction des risques de l'organisme. Il existe également d'autres risques liés aux amendes et aux accusations pénales.

RISQUES LIÉS À LA RÉGLEMENTATION ET À LA CONFORMITÉ

L'industrie des soins de santé est particulièrement vulnérable aux atteintes aux données personnelles en vertu du type de données qu'elle collecte. Les organismes de soins de santé sont terriblement mal préparés aux cyberattaques et aux atteintes aux données personnelles. Les lois relatives à la confidentialité étant gérées au niveau provincial, les organismes doivent s'assurer qu'ils sont en conformité avec les exigences législatives et réglementaires afin d'éviter les amendes et les pénalités.

CONCLUSION

Dans le monde en constante évolution des soins de santé, la technologie et l'innovation ont toujours fait partie de l'équation. Les implications potentielles d'une cyberattaque ou d'une atteinte aux données n'ont toutefois pas encore été complètement appréhendées et quantifiées. Grâce à la récente affaire Hopkins contre Kay (qui a donné naissance au délit d'« atteinte à la vie privée »), les patients peuvent dorénavant intenter un procès civil en raison de préjudices découlant d'atteintes à la confidentialité. Cette affaire peut ouvrir les vannes de futures actions.

Les organismes de soins de santé sont responsables de s'assurer qu'une stratégie de gestion de risques adéquate est au point afin de se protéger au mieux contre les risques mentionnés ci-dessus, pouvant être dévastateurs pour les finances et la réputation. Enfin, cela les aiderait à remplir leur principale obligation : protéger leurs patients. Marsh Canada occupe une position unique pour aider les organismes à examiner et à évaluer leurs stratégies d'atténuation des risques et leur offrir des services-conseils sur les produits et services destinés aux organismes de soins de santé pour gérer ces risques.

Pour en savoir plus, communiquez avec votre représentant Marsh local ou visitez le site www.marsh.ca.

10 Benchmark Study on Patient Privacy and Data Security, Ponemon Institute 9 nov. 2010, http://www2.idexpertscorp.com/resources/healthcare/ healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/#.

USDG-8385 (C150410KB) : 2015/04/27