www.globalsecuritymag.fr

Date : 12/12/2014

Annie Chailan, Chef de marché Santé de Wooxo : Le Big Data appliqué à la Santé : au-delà des opportunités, quels risques liés à la sauvegarde des données ?

Par : Annie Chailan

Si l'essor du Big Data offre une multitude d'opportunités dans le domaine de la santé (recherche médicale, pharmaco-épidémiologie, suivi des pathologies, amélioration des soins, etc), la richesse des données patients expose désormais les établissements qui les exploitent à des risques majeurs liés à l'ultra-sensibilité et à la volumétrie exponentielle de ces données. Aussi la question se pose-t-elle pour les établissements de santé du choix de la solution de stockage et de sauvegarde de ces données, afin qu'elle soit la plus adaptée à leurs problématiques (sécurité, coûts, infrastructures, continuité d'activité).

Le Big Data dans la Santé ouvre de nouvelles perspectives pour la recherche médicale, le suivi des pathologies et l'amélioration des soins

Avant même « l'avènement » du Big Data, l'intérêt d'une veille sanitaire issue de la collecte de données patients avait mené à la création, par exemple, du Réseau Sentinelles en France. Depuis 1984, ce réseau de près de 1300 médecins permet de constituer des bases de données sur plusieurs maladies grâce à la description de cas individuels vus en consultation. En toute logique, l'explosion des datas aujourd'hui décuple ce potentiel.

Quels types de données ?

Selon le rapport McKinsey de janvier 2013 , on retient quatre catégories de données de santé : les données R&D d'entreprises pharmaceutiques ou académiques (ex : essais cliniques), les données cliniques d'hôpitaux figurant dans les Dossiers Patients Informatisés (DPI), les rapports d'activité et données de coûts issus des Caisses d'Assurance Maladie, et les données liées aux comportements

des patients (préférences consommateur, historiques d'achats, activités sportives « connectées », etc).

Quelles avancées ?

Le Big Data est d'ores et déjà prometteur pour la recherche médicale car il permet de traiter des données sur des échantillons cliniques plus grands. De surcroît, couplé à l'internet des objets (bracelets traqueurs d'activités, balances connectées, etc), les données peuvent être recueillies dans des conditions réelles tenant compte du comportement humain. Dans le domaine de la pharmacologie ou de l'épidémiologie, cela permet ainsi de mieux analyser voire prédire certaines épidémies (ex : Google FlueTrends, sur la base des mots-clés recherchés sur Google, est conçu pour anticiper l'évolution d'une épidémie), ou encore d'analyser certains signaux faibles dans le cas de maladies rares , grâce à la large quantité d'échantillons disponibles. De nombreuses opportunités existent également dans le suivi de pathologies comme le diabète ou les défaillances cardiaques : des lecteurs de glycémie ou des pacemakers connectés permettraient au médecin traitant de consulter les données recueillies au quotidien lors des consultations.
Si les opportunités sont multiples, les établissements de santé, quant à eux, doivent faire face à des enjeux liés à l'accessibilité et à l'exploitation de ces données patients.

Les enjeux : une forte volumétrie à gérer, un cadre législatif strict et des données ultra-sensibles

Aujourd'hui le Big Data est un réel enjeu dans la Santé. Les DPI étant de plus en plus volumineux (fichiers d'imagerie médicale, comptes-rendus,...), les établissements de santé sont confrontés à des enjeux technologiques liés au stockage et au partage de ces données entre professionnels voire entre établissements. C'est le principe d'interopérabilité, les établissements de santé doivent pouvoir communiquer entre eux. Se pose ainsi la question du stockage dans le cloud, sur des serveurs sécurisés, mais tributaires du bon fonctionnement du réseau internet et d'une capacité de bande passante suffisante. Les établissements de santé, qu'il s'agisse de cliniques ou de CHU, présentent tous une dépendance accrue à l'informatique. Deuxième enjeu de taille : le cadre législatif. La confidentialité des données de santé et le respect du secret médical requièrent qu'aucun tiers ne puisse accéder à des données médicales, ce qui nécessite d'encrypter les données lorsqu'un réseau internet entre en jeu (clé d'encryption AES 256 imposée par le Code de la Santé Publique). La Certification V-IV de la Haute Autorité de Santé (HAS) normalise quant à elle toutes les actions à mener par les chefs d'établissements de soin (avec audits réguliers) : niveau de sécurité et plan de continuité d'activité notamment. Un hôpital ne peut ni perdre des données, ni s'arrêter de fonctionner ! Et enfin, les établissements doivent satisfaire les prérequis du Projet Hôpital Numérique (Identités et mouvements des patients, Plan de Reprise d'Activité, Confidentialité).

Face à l'ultra-sensibilité des données patients, généralement soumises au secret médical, la notion de sécurité est devenue le nerf de la guerre.
Les risques de piratage et de fuites de données de santé sont omniprésents Piratages, négligences ou erreurs humaines, vulnérabilité des objets connectés aux cyber attaques, sont autant de sources de fuites de données confidentielles contre lesquelles les établissements de santé doivent se prémunir. Si les données patients attirent les pirates informatiques, c'est qu'elles s'avèrent lucratives dans des pays où les traitements sont difficilement abordables pour des personnes dépourvues

d’assurance maladie, comme les Etats-Unis par exemple . Des sociétés peuvent également subir le chantage de pirates informatiques. Ce fut le cas de Mensura, un service de médecine du travail belge, avant que les données ne soient finalement divulguées sur internet . Au-delà de la malveillance d’une cyber attaque, les fuites de données s’expliquent souvent par des négligences humaines et un manque de jugement sur ces questions de sécurité (recours à des hébergeurs de données non agréés par le Ministère de la Santé, par exemple). Avec la multiplication des terminaux nomades, le développement du travail en mobilité et le BYOD (« Bring Your Own Device »), la mobilité devient également un facteur de risque, puisque qu’une tablette ou un smartphone peuvent aisément être perdus ou volés. Pour tirer parti de toutes les opportunités offertes par le Big Data de manière sécurisée, les établissements de soin doivent arbitrer entre des solutions en local ou externalisées dans le cloud pour leurs Plans de Reprise d’Activité (PRA).

Les baies numériques sécurisées, une solution en local sur-mesure répondant aux problématiques des DSIH et des PRA.
Si l’on tient compte des enjeux liés à l’exploitation des données de santé (volumétrie, cadre législatif, ultra-sensibilité) et des risques de fuite de données existants, les chefs d’établissements de santé envisagent traditionnellement les deux possibilités suivantes pour leur PRA :

Dans le cloud : Les établissements peuvent faire le choix du cloud pour leur PRA et sauvegarder leurs données sensibles à distance via des sociétés agréées hébergeurs de données de santé à caractère personnel (article L.1111-8 du Code de la Santé Publique). Cela reste toutefois difficile et compliqué au regard de la volumétrie des fichiers (variabilité des capacités de bande passante, coûts). Cette dépendance à un réseau internet, qui pourra difficilement satisfaire l’impératif de continuité d’activité du Projet Hôpital Numérique, limite ainsi l’intérêt d’une solution Cloud. Néanmoins, le Cloud permet une sécurité maximisée pour le DPI et les données les plus sensibles.

En local classique : Pour cela, les établissements de soins disposent traditionnellement d’un PRA composé de deux « salles blanches » synchronisées pour sécuriser leurs données contre des sinistres physiques (incendies, inondations, etc), l’une prenant le relai de l’autre en cas de crash. La première sera sur le site principal, la seconde dans un bâtiment différent pour assurer la continuité de l’activité de l’établissement. La sauvegarde en local s’affranchit ainsi des contraintes de bandes passantes et assure une reprise d’activité immédiate en cas de sinistre, tout en permettant de contrôler son budget (à la différence des forfaits au Go variables pour un stockage dans le cloud).

En local, avec des coffres-forts numériques : Le coût de mise en place de ces deux « salles blanches » est une réelle contrainte. Il est impératif que ces deux salles soient connectées pour assurer la reprise d’activité en cas de sinistre et la mise en place de fibres optiques. Ce qui implique des contraintes de distanciation entre les deux salles pour parer aux risques d’incendie de grande ampleur ou de catastrophe naturelle. Une baie numérique adaptée à la protection des SIH et des données patients, offre une alternative intéressante en combinant la sécurité d’une véritable salle blanche informatique (ignifuge, étanche, antichoc, climatisée et protégée contre le vol et la malveillance) à la flexibilité d’une approche sur-mesure en termes de coûts et de capacité. Avec des capacités allant jusqu’à plusieurs dizaines de To, les baies numériques hautement sécurisées remplacent efficacement l’une des deux salles blanches, pour un coût sept à huit fois moins élevé à caractéristiques équivalentes.