

La e-santé ne pourra-t-elle bientôt plus se passer du cloud ?

En seulement quelques années, le cloud s'est imposé pour les acteurs de la santé comme une nécessité. Que peut-on aujourd'hui attendre de cette technologie ? Maddyness fait le point avec Emmanuel Meyrieux, chef de projet conformité OVH Healthcare.

Temps de lecture : minute

21 mars 2019

Depuis plusieurs années, le cloud fait partie intégrante de votre quotidien. Il permet des choses variées, comme la sauvegarde de vos contacts téléphoniques et un accès sécurisé à vos photos personnelles. Et cette adoption massive du cloud se retrouve également dans le monde professionnel : celui-ci n'est désormais plus réservé à une élite d'acteurs technologiques. Toutes les entreprises, quel que soit leur secteur ou leur taille, tendent à l'adopter pour une part plus ou moins large de leurs besoins. Aucun secteur n'y échappe... même pas celui de la santé, pour lequel les données s'avèrent hautement sensibles.

" Les établissements de santé, acteurs majeurs du secteur, ont d'abord utilisé le cloud computing internalisé dans leurs propres salles blanches. Ils se montraient particulièrement prudents avant de confier leurs données à des entités extérieures ", explique Emmanuel Meyrieux, chef de projet conformité OVH Healthcare, avant de préciser : " Nous menons un travail de pédagogie au quotidien, tant pour expliquer la technologie cloud que les conditions requises pour assurer un niveau de sécurité optimal des données ".

Des avantages non négligeables

Un travail qui semble avoir porté ses fruits. Encouragés par le passage de plusieurs autres industries au cloud externalisé, de nombreux professionnels de la santé ont finalement, eux aussi, passé le cap. Il faut dire que les bénéfices de la technologie se sont rapidement imposés à eux : les problèmes matériels n'ont plus d'impact sur le système d'information, l'ajout temporaire ou permanent de serveurs ou de mémoire se fait en quelques clics, les besoins d'investissement en informatique sont limités et seules les ressources informatiques consommées sont facturées (au mois)... En externalisant la gestion de l'infrastructure informatique vers un fournisseur de cloud, les entreprises de ce secteur peuvent, à l'instar d'autres secteurs, libérer leur propre personnel technique pour se concentrer davantage sur leur cœur de métier.

Le cloud computing facilite par ailleurs la collaboration entre professionnels de santé sur différents sites en accélérant les projets de dématérialisation des documents. Par exemple, la collaboration à distance de médecins sur des plans de traitement personnalisés de patients devient beaucoup plus efficace. De même que l'exploitation de données dans le cadre d'analyses en santé publique, à des fins sanitaires ou économiques. L'instantanéité d'accès et la facilité de traitement de ces importants volumes de données représentent un moyen d'observer l'émergence et/ou l'évolution des affections à grande échelle pour ensuite mieux les prendre en charge.

Et la sécurité dans tout ça ?

La sécurité des données reste une préoccupation majeure pour l'ensemble du secteur. Les impacts de la perte de données (par exemple du fait d'un *ransomware*, ou rançongiciel en français) ou pire, du vol de celles-ci, peuvent être critiques tant pour le suivi du patient que pour la

réputation de l'établissement concerné. Garder les données loin de tout manquement de sécurité constitue une priorité. Des pirates pourraient-ils compromettre la technologie cloud et accéder aux informations des patients ?

" Les solutions basées sur le cloud ont atteint un stade où elles sont plus sécurisées que les solutions sur serveur local (on premise) ", précise Emmanuel Meyrieux. " Le cloud est constitué de couches supplémentaires de sécurité : la disponibilité et l'intégrité des infrastructures et des données sont mieux assurées grâce à des mécanismes de redondance. La confidentialité reste quant à elle une responsabilité majeure impliquant l'ensemble des parties prenantes, du professionnel de santé au fournisseur d'infrastructure, en passant par l'éditeur de l'application. "

La réglementation force l'ensemble des fournisseurs d'hébergement de données de santé à adopter les meilleures pratiques en matière de sécurité de l'information. Ceci implique une certification et un contrôle annuel de conformité. Ainsi, les données sont aujourd'hui potentiellement mieux protégées chez un prestataire externe qu'au sein même de l'établissement de santé, qui n'est pas forcément soumis aux mêmes contrôles.

L'avènement des technologies de cloud computing a renforcé l'intérêt de solliciter des fournisseurs spécialisés, à l'instar du français OVH, dont le métier est d'investir dans des infrastructures performantes et sécurisées, au meilleur coût pour les clients. Fin 2016, OVH obtenait d'ailleurs l'agrément d'Hébergeur de Données de Santé (HDS). Il lançait alors son offre OVH Healthcare afin de fournir aux acteurs de la santé des datacenters virtuels fonctionnant sur les outils VMware, et disposant de toutes les fonctionnalités de gestion automatisée. Son credo : *" Nous ne savons pas traiter les patients, mais nous prenons soin de nos infrastructures ! "*

Des limites à dépasser

Alors, qu'est-ce qui retient encore les acteurs de la santé ? La simple idée de passer à un système entièrement dématérialisé peut, encore aujourd'hui, décourager des professionnels habitués depuis des décennies à conserver la maîtrise complète de leur système d'information.

" Dans le secteur de la santé, les données sont encore trop souvent fragmentées, incomplètes, cloisonnées et pas interopérables ", se désole Emmanuel Meyrieux. " Ces organisations ont compris que pour fournir des soins de pointe à des coûts raisonnables aux patients, ils devront pouvoir s'appuyer sur des données fiables et disponibles en temps réel. C'est l'objectif prioritaire de la majorité des éditeurs de logiciels de santé aujourd'hui, qu'ils existent depuis longtemps ou qu'ils commencent comme startups ", conclut-il.

Maddyness, partenaire média de OVH.