NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Pourquoi le cloud souverain et de confiance est-il un atout majeur pour le secteur de la santé ?

Résumé

- Le secteur de la santé fait face à de grands défis en matière de **transformation numérique** : **exigences opérationnelles** pour fournir des soins de bonne qualité aux patients, accélération de la recherche...
- En parallèle, la **donnée de santé** n'a quant à elle jamais été aussi convoitée.
- La donnée de santé se doit donc d'être **confidentielle** dans le **respect de la vie privée** de chacun mais avant tout pour les professionnels de santé, elle se doit d'être **intègre** (sans risque de corruption, de modification de la donnée) et **disponible en permanence**, à l'instant où elle se révèle nécessaire, parfois pour des questions d'urgence vitale.

Les données médicales : sensibles, confidentielles et donc à protéger

- **Qu'est-ce que sont les données de santé ?**

Les données de santé font partie des catégories particulières de données au sens de l'article 9 du RGPD. Ce sont des données dites sensibles qui nécessitent un niveau de protection élevée. Une donnée de santé est souvent numérique mais pas uniquement : elle peut être archivée sous la forme d'un écrit de type certificats médicaux, résultats d'analyse... ou sous la forme d'enregistrements d'un professionnel de santé dans le cadre de comptes-rendus médicaux, sous forme d'images (imagerie médicale)...

> Les données de santé, un trésor très convoité…

Un dossier médical peut se revendre entre 50 et 100 dollars sur le dark web, soit en moyenne trois fois plus cher que des données classiques à des fins multiples, comme la recherche médicale. La compromission de données telles que les problèmes de santé passés et présents, les ordonnances de pharmacie, les dossiers d'hôpital, les détails sur les assurances, peuvent permettre de se faire passer pour un médecin et ainsi escroquer l'Assurance Maladie en demandant des remboursements injustifiés. On assiste également de plus en plus au « chantage à la personne », soit de personnes privées menacées de diffusion d'informations médicales les concernant, permettant de détecter une pathologie ou encore de personnes publiques, comme la diffusion d'informations sur l'état de santé d'un dirigeant d'un pays.

> Quels sont les avantages du cloud vs les infrastructures on premise ?

Le développement des usages numériques, la nécessité de proposer un parcours patient de plus en plus fluide, de pouvoir faire face à des pics d'activité ou encore à des épidémies, la nécessité impérieuse de se prémunir contre des cyberattaques, le développement de l'usage des solutions d'IA générative… Autant de raisons qui militent pour des infrastructures mobilisables à la demande, à la pointe de la sécurité, conformes aux règlementations… ce que permet le cloud.

> Les établissements de santé, une cible très exposée aux cyberattaques

En Entre janvier 2021 et mars 2023, l'Agence de l'Union Européenne pour la Cybersécurité (European Union Agency for Cybersecurity, Enisa) a dénombré 215 incidents (principalement des cyberattaques). Sont concernés : les hôpitaux, les laboratoires, les mutuelles, les organismes publiques de santé ou encore les industries pharmaceutiques. C'est le secteur le plus attaqué et de loin. En effet, avec plus d'une cyberattaque sur deux concernant le domaine de la santé (53% précisément) et la France est le pays le plus touché (sources : étude 2023 de l'Agence Européenne de Cybersécurité). Les conséquences de ces cyberattaques se révèlent la plupart du temps dramatiques à court moyen et long terme. Le recours au cloud souverain et de confiance pour l'hébergement et la protection de ses données est une voie à privilégier pour pallier ces cyberattaques, mettre en place des dispositifs de reprise d'activité rapide et se mettre en conformité avec les nombreuses règlementations. Plus largement, le recours au cloud permet d'externaliser le système d'information et ainsi d'accélérer la modernisation et la transformation, sans avoir à investir en interne sur des ressources dédiées.

> Le cloud souverain et de confiance, la garantie de conformité règlementaire pour le secteur de la santé

L'obligation règlementaire HDS

Régies par le secret médical, les informations des patients doivent être archivées et traitées dans un cadre de sécurité renforcée. Seuls les prestataires certifiés HDS (Hébergeur de Données de Santé) peuvent héberger les données médicales. Les structures publiques ou privées souhaitant traiter des données médicales à caractère personnel doivent donc faire appel à un prestataire labellisé HDS en vue de garantir le respect de la vie privée des patients. Le label est-il suffisant pour héberger les données de santé ? La réponse n'est pas si simple et dépend des données dont on parle.

Pourquoi privilégier un cloud souverain et de confiance pour l'hébergement de ses données de santé ?

Par « souverain », on entend l'hébergement et l'ensemble des traitements effectués sur des données physiquement réalisés dans les limites du territoire national par une entité de droit français/européen et en application des lois et normes françaises/européennes. Les lois extraterritoriales ne peuvent donc s'appliquer et la conformité RGPD est garantie.

Pour rappel, les hyperscalers américains sont soumis au **« Cloud Act »** et à la **loi Fisa** qui indique en substance que des réquisitions peuvent être faites par le gouvernements américains à tout moment et cela sans avertissement préalable. En parallèle, le **règlement RGPD** stipule que les données personnelles ne peuvent être transférées, exploitées... sans le consentement éclairé de la personne.

Par **« de confiance »**, on entend que l'hébergement en plus d'être souverain est soumis aux plus hauts standards de sécurité en matière de cloud, à savoir la qualification SecNumCloud.

Le législateur lui-même stipule que la qualification SecNumCloud est à privilégier de manière directe dans la circulaire **« cloud au centre »** de mai 2023 : celle-ci impose aux acteurs du secteur public qui ont recours à un cloud public que les données protégées par la loi (délibérations de l'État, défense, sécurité nationale, santé, données personnelles...) soient hébergées dans un cloud SecNumCloud.

Mais tout autant de manière indirecte, dans le cadre de **NIS2**, qui concerne un grand nombre d'acteurs du secteur de la santé en tant qu'EE (Entités Essentielles) ou EI (Entités Importantes).
Cette règlementation a pour but de renforcer la cybersécurité des réseaux et des systèmes d'information au sein de l'Union européenne,
elle impose des obligations en matière de cybersécurité, de déclaration d'incidents...

La conformité des organisations est attendue pour octobre 2024, au-delà de cette date l'ANSSI pourra procéder à des audits et appliquer des sanctions en cas de non-conformité. La qualification SecNumCloud permet de couvrir un grand nombre de ces obligations.

Le cloud souverain et de confiance comme rempart aux cyberattaques, solution résiliente et de reprise d'activité

Parmi les avantages comparatifs du cloud de confiance :

1 Ressources expertes

Les fournisseurs de services cloud disposent d'équipes dédiées de professionnels de la sécurité informatique qui travaillent en permanence pour protéger les données de leurs clients contre les attaques. Ils utilisent des technologies avancées, telles que l'analyse comportementale et l'apprentissage automatique, pour identifier les menaces potentielles et y répondre rapidement.

2 Certifications et qualifications

Les fournisseurs de services cloud investissent massivement dans des certifications de sécurité, comme la norme ISO 27001, le standard SecNumCloud délivré par l'ANSSI ou encore le standard HDS dans le secteur de la santé, prouvant leur engagement et leurs compétences en matière de cybersécurité.

3 Gestion des accès

Des outils de gestion des identités et des accès sont développés pour garantir que seules les personnes habilitées ont accès aux données autorisées. Ces outils permettent aussi de suivre les activités des utilisateurs, détecter les comportements suspects, et réagir rapidement aux menaces potentielles.

4 Chiffrement et authentification

Le chiffrement convertit les données en un code ininterprétable pour les personnes non autorisées. Il est utilisé pour garantir la confidentialité des données stockées dans le cloud. Les systèmes d'authentification incluent des mots de passe, des codes PIN, des clés de sécurité ou des systèmes de reconnaissance biométrique, pour restreindre encore plus largement l'accès aux données à qui n'est pas autorisé.

5 Résilience

Les fournisseurs de services cloud disposent de technologies de sauvegarde et de récupération pour garantir la disponibilité des données en cas de perte ou de corruption des systèmes. Des centres de données redondants pour stocker les données dans des emplacements géographiques différents sont déployés, garantissant ainsi la disponibilité des données en cas de panne ou de catastrophe naturelle par exemple.

Point de vigilance toutefois :

Le cloud offre indéniablement de très bonnes garanties en matière de cybersécurité, assure une haute disponibilité des données et réduit les risques de perte de confidentialité. Néanmoins, lorsqu'une entreprise utilise un environnement cloud pour exécuter ses applications, elle est responsable de la sécurité de ses applications : elle doit donc prendre des mesures de sécurité pour protéger ses applications contre les cyberattaques. En cas d'infection des applications, c'est tout l'environnement cloud qui peut se trouver infecté et attaqué.

Point de vigilance toutefois : **le cloud offre indéniablement de très bonnes garanties en matière de cybersécurité**, assure une haute disponibilité des données et réduit les risques de perte de confidentialité. Néanmoins, lorsqu'une entreprise utilise un environnement cloud pour exécuter ses applications, elle est responsable de la sécurité de ses applications : elle doit donc prendre des mesures de sécurité pour protéger ses applications contre les cyberattaques. En cas d'infection des applications, c'est tout l'environnement cloud qui peut se trouver infecté et attaqué.

Le cloud permet d'adresser bon nombre de défis en matière de santé :

- **Il facilite l'accès aux données de santé…**
  … en fournissant des outils d'analyses pratiques qui facilitent l'accès aux informations, une excellente gestion des données de façon sécurisée et en conformité avec les règlementions en vigueur. En réalité, le cloud computing est une solution informatique particulièrement adaptée au secteur de la santé, car il permet le stockage des données, l'accès sécurisé aux différentes parties prenantes ainsi que l'exécution de logiciels métier de façon performante.

- **Il améliore la communication entre les professionnels de santé**
  En améliorant la collaboration entre les professionnels de santé, quel que soit le lieu où se trouve le praticien, le cloud permet de transmettre à ses pairs et collègues des informations collectées sur place. Ceci permet également de réduire les dépenses de santé en évitant de refaire des examens déjà réalisés.

- **Il permet d'améliorer la collaboration patient-médecin**
  Le patient peut aisément se servir du cloud pour partager certaines informations avec le professionnel de son choix sur son état de santé. Si le patient ne peut se déplacer jusqu'à un hôpital, le Cloud permet d'optimiser le suivi des patients à distance, grâce notamment aux pratiques de télémédecine ou de téléversement des données des dispositifs médicaux de mesure labellisés, conformément aux directives européennes qui se développent de plus en plus, car il réduit drastiquement les erreurs dans les traitements. Avec la rapidité de l'accès à l'information et du partage des documents en ligne, le cloud permet aussi de réduire le temps d'hospitalisation des patients dans les hôpitaux.

- **Il contribue à l'amélioration de la recherche médicale**
  La fonction première du cloud est le stockage en ligne et le partage des données. Les « Data analysts » du domaine de la santé peuvent se baser sur le cloud pour condenser et analyser des données complexes.

- **Il accélère la prise en charge du patient et permet de se consacrer à l'essentiel**
  L'IA et l'IA générative ont de nombreuses applications dans le domaine de la santé. L'exemple de l'IA générative souveraine Medassistant** est un exemple parlant. Cette application permet aux professionnels de santé qui prennent en charge des patients à pathologies lourdes et complexes ayant un dossier médical conséquent de bénéficier d'une synthèse qualitative et fiable de l'ensemble des éléments figurant dans le dossier médical, pour se concentrer sur la recherche du meilleur protocole de soins à mettre en place.

Contactez-nous

Nathalie Dufouil, Responsable Secteur Santé
nathalie.dufouil@numspot.com

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous

@NumSpot
@NumSpotCloud