Données de santé : l'hébergement souverain n'est plus une option

Alors que l'État accélère sa sortie des dépendances numériques extra-européennes, les établissements de santé ne peuvent plus différer leurs choix d'hébergement. Derrière les enjeux techniques, c'est la protection des données patients qui est en jeu. Entre risques juridiques, exigences de conformité et pression des régulateurs, s'appuyer sur un hébergeur HDS souverain s'impose comme une condition de confiance.

Un tournant réglementaire structurant

Le 8 avril 2026, la DINUM réunissait ministères, opérateurs publics et industriels pour accélérer cette transition. La Plateforme des données de santé migre le SNDS vers un cloud SecNumCloud, non soumis aux législations étrangères. Une première copie est attendue fin 2026.

Pour les DSI et RSSI hospitaliers, le message est clair : la souveraineté est une exigence immédiate. Elle conditionne la capacité à répondre aux contrôles, sécuriser les systèmes et protéger les données patients.

Le CLOUD ACT, un risque juridique incompatible avec les exigences de santé

Recourir à des prestataires soumis à des juridictions extra-européennes expose les données à des réquisitions extrajudiciaires via le CLOUD ACT. Une contradiction directe avec le RGPD et le référentiel HDS.

La complexité des chaînes de sous-traitance aggrave le problème. Intermédiaires multiples, infrastructures tierces, accès difficiles à tracer : autant de facteurs qui fragilisent la maîtrise des données. En cas d'incident, cette opacité devient critique.

Repenser l'architecture d'hébergement comme levier de maîtrise

La souveraineté ne se limite pas à la localisation des données. Elle implique une maîtrise complète de la chaîne, de l'infrastructure à la gouvernance des accès.

Garantir disponibilité, intégrité et confidentialité suppose des choix d'architecture qui intègrent les risques juridiques dès le départ. La conformité devient un résultat, non un point de départ.

Des choix d'hébergement qui ne relèvent plus de l'option

Le marasme actuel lié aux enjeux géopolitiques implique de sortir de l'attentisme qui s'était largement étendu autour des enjeux de souveraineté et de sécurité. Structurer une stratégie d'hébergement souverain, c'est sécuriser les données, garantir la conformité et anticiper les contrôles. Les établissements doivent démontrer leur maîtrise.

Les solutions retenues doivent offrir des garanties concrètes : indépendance vis-à-vis des juridictions extraterritoriales, solutions d'hébergement open source, transparence contractuelle, traçabilité des opérations. La souveraineté est désormais un prérequis.

gplexpert : un hébergeur français certifié et sans dépendance

gplexpert apporte une réponse opérationnelle et immédiatement mobilisable.
Datacenters localisés en France, exploitation en propre, actionnariat exclusivement français : une indépendance totale vis-à-vis de toute législation extraterritoriale.

Les certifications ISO 27001 et HDS structurent cette exigence. Traçabilité complète des opérations, lisibilité contractuelle, gouvernance simplifiée.

Avec gplexpert, la souveraineté devient une réalité vérifiable, à chaque niveau, pour chaque audit.

« Après trente ans à accompagner des établissements de santé dans leur transformation numérique, je constate que la question n'est plus faut-il migrer vers un hébergement souverain ? mais combien de temps peut-on encore attendre ? Ce constat fait écho à des choix structurants engagés dès 2008, notamment le virage vers l'open source, qui s'est révélé un pari durablement gagnant en matière de maîtrise et d'indépendance. Les régulateurs ont fixé le cap. Les établissements qui ont anticipé cette transition ne gèrent plus des risques, ils construisent de la confiance. La souveraineté numérique s'impose aujourd'hui comme un socle essentiel pour concilier performance, conformité et responsabilité dans le secteur de la santé. »

Thomas Breton, Fondateur gplexpert