SYNOVO GROUP
IT & SOFTWARE SOLUTIONS

Professionnels de santé : pourquoi choisir un éditeur de logiciel certifié HDS sur les 6 niveaux ?

HÉBERGEUR DE DONNÉES DE SANTÉ — HDS

INFOGRAPHIE

Pour respecter une obligation légale
en vigueur depuis juin 2018

JUIN 2018

Depuis juin 2018, l'ANS (Agence du Numérique en Santé) oblige les entreprises manipulant des données de santé à être conformes au référentiel « Hébergeur de Données de Santé ». **Ainsi, pour l'externalisation des données, elles doivent obligatoirement travailler avec un hébergeur certifié, choisi parmi ceux listés par l'ANS.**

Découvrir la liste de l'ANS

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

Pour bénéficier de
nombreuses garanties

Garanties de sécurité

Les éditeurs certifiés HDS doivent proposer à leurs clients des aspects contractuels très cadrés en terme de sécurité.

Garantie de disponibilité

Les éditeurs doivent disposer de garanties d'accès à leurs logiciels / applications. Les pannes doivent être maîtrisées afin de garantir un niveau de disponibilité optimal.

Garantie de non utilisation des données à des fins marketing

Les données à caractère personnel sont traitées uniquement pour la bonne exécution des services. Aucune utilisation commerciale n'est autorisée.

Garantie de temps de rétablissement

L'éditeur est préparé à d'éventuelles attaques et dispose de procédure **de continuité et de gestion des incidents** afin de les résoudre de la manière la plus optimale.

Pour sécuriser les données stockées
dans vos logiciels métier

Les données de santé sont des informations très sensibles et critiques. **Elles sont très recherchées par les cyberattaquants car elles sont plus rémunératrices que de simples données personnelles.** Ainsi, les éditeurs de logiciels certifiés HDS se doivent de sécuriser les données stockées dans leurs logiciels en respectant des référentiels. Ci-dessous quelques exemples*.

1 — 2 — 3

Les noms des patients sont **remplacés par des identifiants uniques**.

Les données personnelles de vos patients sont masquées : votre éditeur n'a pas à y avoir accès.

Des analyses de risques sont régulièrement effectuées pour renforcer la sécurité de votre éditeur.

** Liste non exhaustive*

Pour capitaliser sur un prestataire
qui fait évoluer ses process de sécurité continuellement

1 — 2 — 3

Un niveau de sécurité en constante croissance : des audits externes sont réalisés périodiquement pour vérifier l'évolution constante des process de cybersécurité.

Des employés régulièrement sensibilisés afin de les rendre attentifs aux risques liés à la cybersécurité. Un employé averti en vaut deux, notamment pour la prévention, la détection et la réaction.

Une équipe à l'écoute, mettant en place des conseils **pour aider ses clients dans la mise en place d'une politique de sécurité cohérente**.

Pour respecter et couvrir toute
la chaîne de sécurité

Votre éditeur doit être certifié HDS sur les 6 niveaux afin de couvrir les 3 activités suivantes :

L'infogérance

Les sauvegardes externalisées

La sécurité du Data center

Dans le cas contraire, il existe alors une rupture de la chaîne de sécurité et votre activité n'est pas conforme au réfentiel de sécurité exigé par la certification HDS.

Pour plus d'informations,
prenez contact avec notre équipe !

EN SAVOIR PLUS