# LEGAL FLASH

## Vous hébergez des données de santé ? Vous êtes concernés !

### 1 Rappel sur la qualification de HDS et mes obligations en découlant

- Selon le le Code de la santé publique : toute personne qui **héberge des données de santé à caractère personnel** recueillies à l'occasion d'activité de prévention, diagnostic, soins ou suivi social et médico-social pour le compte de personnes à l'origine de la production ou du recueil de ces données
- L'hébergement peut être sur **papier** ou **numérique** et fait l'objet d'un contrat
- Les hébergeurs ne peuvent **utiliser les données confiées qu'aux fins de la prestation d'hébergement**
- Toute **cession** des données de santé identifiantes est interdite
- Les hébergeurs sur support numérique doivent être titulaire d'un **certificat de conformité**
  - ➢ Le référentiel d'accréditation HDS publié par l'agence du numérique en santé liste des exigences pour répondre aux obligations du certificat de conformité

### 2 Les exigences issues du nouveau référentiel

- Précision sur l'activité d' « *administration et exploitation du système d'information contenant les données de santé* » : il s'agit de la **maîtrise des interventions sur les ressources mises à la disposition du client de l'hébergeur**
- Précision sur **l'articulation entre la certification HDS et celle SecNumCloud** de l'ANSSI
- Intégration de certaines évolutions de la **norme ISO 27001**
- 4 nouvelles exigences quant à la souveraineté des données :
  - ➢ Les données doivent **être physiquement hébergées au sein de l'EEE**
  - ➢ En cas d'accès distant par l'hébergeur ou ses sous-traitants depuis un pays hors EEE, l'accès doit être fondée sur une **décision d'adéquation de la Commission européenne ou une garantie du RGPD** et l'HDS doit en informer le client
  - ➢ Si l'HDS est soumis à une législation d'un pays qui n'assure pas une protection adéquate : indiquer la **règlementation de ce pays autorisant celui-ci à avoir un accès non autorisé aux données, les mesures prises pour atténuer le risque d'accès non autorisé et la description des risques résiduels**
  - ➢ L'hébergeur doit **rendre publiques et tenir à jour les informations sur les transferts de données vers des pays hors EEE** et sur **les mesures mises en place pour respecter le RGPD**, notamment via une cartographie

➔ **Entrée en vigueur prévue au deuxième semestre 2024**

TROIS QUATORZE
Lyon • +33 (0)6 83 25 34 63 • troispointquatorze.fr
valerie.chazaud@troispointquatorze.fr