L'ECLAIRAGE DU MARDI

par

COMETH CO CONSULTING

## Hébergement de données de santé

**Mardi 09 avril 2019**

**Qu'est-ce qu'une donnée de santé ?**
Alors que la Loi Informatique et libertés de 1978 encadrait tous types de données à caractère personnel, mais sans précision pour les données de santé ; le législateur européen a défini dans **l'article 4 du RGPD**, les données de santé comme : « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de service de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

La notion de données de santé est désormais élargie et nécessite d'être appréciée au cas par cas compte tenu de la nature des données recueillies, ainsi **trois types de données** sont identifiés **:**

- Les données de santé **par nature**, telles que : les antécédents médicaux, les maladies, les prestations de soins réalisés, les résultats d'examens ou encore un handicap.
- Les données qui, **du fait de leur croisement**, deviennent des données de santé car elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne, telles que : le croisement de la tension avec la mesure de l'effort (*nombre de pas et mesure des apports caloriques par exemple) ;*
- Enfin, les données qui deviennent des données de santé **en raison de leur destination** (*un numéro de chambre d'hôpital par exemple*) ;

**Comment bâtir un écosystème de confiance autour de la santé numérique ?**
Au vu de leur sensibilité, le stockage des données de santé exige plusieurs conditions[1], dont deux principales :

- Elles doivent être protégées par **un accès sécurisé** afin de respecter le secret médical et ainsi préserver la confidentialité de la vie privée des personnes.

[1] Article L1118-1 du Code de la santé publique

- Il est primordial de conserver **leur intégrité** pour garantir la traçabilité et la qualité des données afin d'assurer un bon niveau des soins.

**Le cadre règlementaire** applicable à **l'Hébergement de Données de Santé à caractère personnel (HDS)** est en évolution constante :

- Il a été établi en France par la loi 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
- Ensuite à travers le décret n° 2006-6 du 4 janvier 2006, l'activité HDS fût subordonnée à l'obtention préalable **d'un agrément**, prononcé pour une durée de 3 ans par le comité d'agrément des hébergeurs (CAH) placé auprès de l'Agence des systèmes d'information partagés de santé (ASIP santé).
- L'ordonnance du 12 janvier 2017, prise en application de la loi de modernisation du système de santé du 26 janvier 2016, a remplacé la procédure d'agrément par **une procédure de certification** délivrée par un organisme certificateur accrédité par le Comité français d'accréditation (COFRAC).
- Le décret 2018-137 du 26 février 2018 définit la procédure de certification et organise **la transition entre l'agrément et la certification**. L'arrêté portant approbation des référentiels d'accréditation et de certification publié le 29 juin 2018 permet l'ouverture du schéma d'accréditation HDS.


*Schéma original ASIP Santé*

**Les projets de certification sont à forts enjeux pour les HDS** (sanctions, réputation, etc.). Ils seront basés sur **un référentiel élaboré par l'ASIP santé** et s'appuyant sur les exigences des normes internationales **ISO 27001** (système de gestion de la sécurité des systèmes d'information), **ISO 20000** (système de gestion de la qualité des services), **ISO 27018** (protection des données à caractère personnel) et **d'exigences spécifiques** à l'hébergement de données de santé.

***Rendez-vous prochainement pour un nouvel éclairage***

COMETH Consulting – 17 rue Charles Laffitte 92200 Neuilly-sur-Seine
www.cometh-consulting.com / contact@cometh-consulting.com / Tél : 01 40 54 83 81