AVIS D'EXPERT

PROVADYS - INFORMATION SECURITY

Joël RAMAT – expert consultant senior Information Security

Le référentiel HDS, source d'inspiration pour des SI conformes au RGPD

Ni la CNIL, ni le Contrôleur européen de la protection des données (CEPD qui prend la suite le G29) ne proposent, à ce jour, de **référentiel** de qualification des systèmes d'information de traitement des données à caractère personnel pour garantir une conformité avec le RGPD.

Néanmoins, d'autres référentiels adressent la sécurité des données et permettent d'être certifié tels que l'ISO 27001 pour les systèmes d'information, PCIDSS pour la protection des données de carte bancaire ou HDS pour la protection des données de santé à caractère personnel que nous vous présentons ci-après.

La certification hébergeur de donnée de santé

La progression de l'externalisation des traitements de donnée dans le cloud a amené l'état à légiférer pour protéger les données de santé des patients en cas d'externalisation des systèmes d'information de santé.

Ainsi le code de santé publique impose d'être certifié HDS (Hébergeur de Données de Santé) à compter du 1er janvier 2019 pour « *toute personne (physique ou morale) qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social , pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même* » (article L.1111-8 du code de la santé publique).

Sont concernés, par exemple :

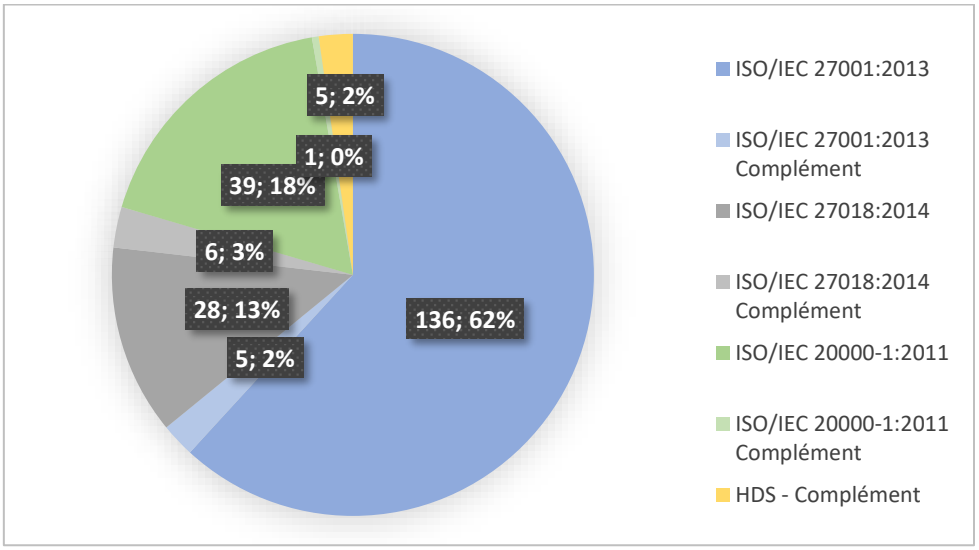
- Les éditeurs de solutions logiciels en mode SAAS (Software As A Service) de suivi de la patientèle ;
- Les prestataires d'infogérance de SIS (Système d'Information de Santé) externalisés ;
- Les prestataires de sauvegardes externalisées dès lors que des données de santé visées par l'article sont concernées ;

- Les GHT (Groupement Hospitalier de Territoire) qui hébergent les SIS des hôpitaux rattachés ;
- Les conseils généraux qui hébergent des systèmes d'information de santé tels que ceux des MDPH (Maison Départemental des Personnes Handicapées) ;
- Tout organisme qui profitait de l'agrément de son hébergeur et qui réalisait à son compte une partie des tâches de gestion et de maintien du SIS.

Sont dispensés, par exemple :

- Les organismes d'assurance maladie obligatoire et complémentaire ;
- Les organismes de recherche dans le domaine de la santé ;
- Les fabricants/fournisseurs/distributeurs de dispositifs médicaux en dehors du cas où ils interviennent dans des activités de télésurveillance ;
- Les associations qui proposent des activités sportives à des personnes handicapées ;
- Les médecins/infirmiers qui hébergent les dossiers de leurs patients au sein de leur cabinet.

Le référentiel HDS possède la particularité d'être constitué d'un agrégat de plusieurs référentiels.



Répartition, dans le référentiel HDS, des exigences par référentiels d'origine

Ainsi, le chapitre 4 « Exigences du référentiel de certification HDS » comprend :

- Les exigences de la norme ISO/IEC 27001:2013 reprise dans son intégralité ;
- Une partie des exigences énumérées dans la norme ISO/IEC 20000-1:2011 ;
- Des exigences complémentaires aux normes ISO/IEC 27001 et ISO : IEC 20000-1 ;
- Des exigences relatives à la protection des données de santé à caractère personnel, identifiées comme exigences principales dans le chapitre 4, pour lesquelles un respect des exigences de la norme ISO 27018 pourra conférer une présomption de conformité ;
- Des exigences relatives à la protection des données de santé à caractère personnel, identifiées comme exigences complémentaires dans le chapitre 4 ;

- Des exigences spécifiques au domaine de la santé tel que la prise en compte de la PGSSI-S (politique générale de sécurité des systèmes d'information de santé) par les clients.

Les exigences sont à adresser en fonction des activités proposées par l'hébergeur. Le tableau suivant présente les différentes activités HDS, les modèles de services d'hébergement type et les responsabilités de traitement.

<table>
<tr><td colspan="2"></td><td>Données de Santé à Caractère Personnel</td><td rowspan="8"></td><td colspan="3">Responsable de Traitements
–
Médecin, Infirmier, Clinique, Hopital, Laboratoire de Biologie Médical
–
Production et Collecte des données de santé</td></tr>
<tr><td rowspan="4">Prestation d'hébergeur infogéreur</td><td>6. Sauvegardes externalisées des données de santé</td><td rowspan="2">Application</td><td rowspan="7">SAAS</td><td rowspan="6">PAAS</td><td>Sous-traitant de Niveau 1
–
Prestataire de service
–
Application de suivi de patientèle</td><td rowspan="6"></td><td rowspan="3">Sous-traitant de Niveau 1
–
Prestataire de service
–
Application de suivi de patientèle ET Plateforme d'hébergement Certifié HDS (3 et 5)</td></tr>
<tr><td>5. Infogérance d' exploitation</td><td rowspan="3">Base de données

Middleware

Système d'exploitation</td><td rowspan="3">Sous Traitant de Niveau 2
–
Hébergeur
–
Plateforme d'hébergement Certifié HDS (1,2,3,4,5)</td></tr>
<tr><td>3. Plateforme logicielle</td></tr>
<tr><td>4. Infrastructure virtuelle</td><td>Virtualisation</td><td rowspan="3">IAAS</td><td rowspan="3">Sous Traitant de Niveau 2
–
Hébergeur
–
Infrastructure d'hébergement Certifié HDS (1,2 et 4)</td></tr>
<tr><td rowspan="2">Prestation d'hébergeurs d'infrastructure physique</td><td>2. Infrastructure matérielle</td><td>Serveur Stockage Réseau</td></tr>
<tr><td>1. Locaux</td><td>Datacenter</td></tr>
<tr><td colspan="2">Activités HDS</td><td colspan="2">Modèle de Services</td><td colspan="3">Responsabilité quant au traitement des DCP</td></tr>
</table>

***SAAS (Software As Service)** : Utilisation d'un logiciel comme d'un service (ex : Office 365, G Suite, Salesforce)*
***PASS (Plateforme As A Service)** : Utilisation d'une plateforme comme d'un service (ex : site web, vous disposez d'un accès sftp et d'un accès à une base de données pour déployer votre site web)*
***IAAS (Infrastructure As A Service)** : Utilisation d'une infrastructure comme d'un service (vous gérez les quantités de ressources/serveurs ainsi que l'OS), peut-être dédié ou mutualisé.*

On peut noter que l'application (hors cas d'un service de sauvegarde externalisé) n'est pas dans le périmètre de l'hébergeur, mais bien de son client qui devra s'engager à respecter la PGSSI-S (Politique Générale de Sécurité des Systèmes d'information de Santé). L'application ne nécessite pas d'être certifiée ou contrôlée par un tiers indépendant.

Transposition au RGPD

Le RGPD est bien sûr à prendre en compte par les différentes parties. Le responsable de traitements est le producteur et collecteur des données de santé. Le prestataire de service sous-traitant qui fournit l'application de traitement doit être certifié Hébergeur de donnée de santé ou faire appel à un sous-traitant de niveau 2 certifié HDS.

Les données de santé sont catégorisées données sensibles par le texte. L'organisme qui souhaitera apporter des garanties de sécurité sur son système d'information ou son offre de service d'hébergement de DCP pourra donc fortement s'inspirer du référentiel HDS.

Cependant, la certification HDS ne traite pas le périmètre applicatif, c'est-à-dire le traitement de données en lui-même. Afin de compléter le dispositif, d'autres référentiels pourront être utiles, par exemple l'OWASP pour la sécurité des applications WEB ou PCI DSS pour la protection des données de carte bancaire.

Enfin, le travail spécifique aux traitements des données personnelles sera toujours à mener :

- Constitution et maintien des registres de traitement (interne et sous-traitance)
- Sélection des données personnelles réellement nécessaires aux traitements
- Analyse d'impact sur les traitements sensibles
- Respect du droit des personnes

Conclusion

Les référentiels certifiants permettant d'adresser la sécurité des données ne manque pas. L'organisme devra choisir ses référentiels de conformité selon ses enjeux, ses objectifs et son niveau de maturité.

L'obtention et le maintien d'une certification engendrent des exigences et des modes de fonctionnement qui ont de réels apports, par exemple en cas de violation de données. Si un tel événement se produit, l'entreprise devra démontrer qu'elle a mis en place les mesures techniques de protection appropriées. La certification lui apportera les éléments de réponses adéquats. En s'appuyant sur le référentiel HDS, les éléments de preuve existent, sont identifiés et accessibles. Il est plus simple de remonter à la source de l'attaque.

Le référentiel HDS apporte une reconnaissance plus forte du niveau de protection des données personnelles qu'une certification ISO 27001. Aussi, HDS sera un vrai gage de confiance auprès de vos clients et usagers qui vous confie leurs données.