L’agrément d’hébergeur de données de santé d’Orange Healthcare

Orange Healthcare a été le premier opérateur à obtenir l’agrément

En France, l'activité d'hébergement de données de santé à caractère personnel de patients est subordonnée à l'obtention préalable d'un agrément délivré par le ministère de la Santé. Les conditions de l'agrément sont fixées par le décret n° 2006-6 du 4 janvier 2006 qui organise la procédure d'agrément et qui fixe le contenu du dossier à soumettre.
L’agrément est attribué après une durée d’instruction de maximum 8 mois, pour une durée de 3 ans reconductible, après avis motivé d'un comité d'agrément (ASIP) et de la CNIL.

Qu’est-ce que l’agrément pour l’hébergeur de données de santé

Champ d’application de la règlementation « hébergeur de données de santé »

Art. L1111-8 du Code de la Santé Publique (CSP), issu de la loi n°2002-303 du 4 mars 2002 (dite « Loi Kouchner ») et modifiée par la loi du 26 janvier 2016 relative aux droits des malades et à la qualité du système de santé, prévoit que :
« Toute personne qui héberge des données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou 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 desdites données ou pour le compte du patient lui-même doit être agréée à cet effet.
Cet hébergement est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. »

Principe

Hébergement des données de santé à caractère personnel auprès d’un prestataire agréé
1/ Pour les données collectées dans le cadre d’activités de prévention, de diagnostic, de soins ou de suivi social et médico-social ;
2/ Pour les données de suivi social et médico-sociales.
Extension introduite par la loi du 26 janvier 2016, mais auparavant la CNIL et le CAH (ASIP Santé) retenait déjà une interprétation large de l’article L.1111-8 du code de la santé publique compte tenu de sa finalité : protéger les bases de données de santé afin de préserver la vie privée des individus.

Exceptions

1/ **Hébergement par le professionnel de santé ou l’établissement de santé** : la réglementation dispense les établissements et les professionnels de santé hébergeant leurs données en local d’obtenir cet agrément pour héberger des données de santé à caractère personnel de leurs propres patients.
2/ **Recherches biomédicales** : sur saisine de l’ASIP Santé, la mission juridique du Conseil d’État auprès du ministère de la Santé a conclu que « les bases de données de santé constituées à l’occasion de recherches biomédicales n’étaient pas soumises à la procédure d’agrément prévu à l’article L1111-8 du code de la santé publique et précisée par le décret 2006-6 du 4 janvier 2006 ». Mais pour l’ASIP Santé, il n’y a pas d’exemption pour les recherches biomédicales.
3/ **Données de wellness/quantified self** : celles qui ne sont pas collectées dans le cadre d’activité de prévention de diagnostic ou de soins sauf si à finalité médicale (envoi à son médecin traitant par exemple).
4/ **Données anonymisées** de manière irréversible.

Secret professionnel

L'hébergeur et les personnes intervenant sur la plateforme d'hébergement sont tenus au secret professionnel.

- « Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreintes au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal. » (al. 10 art. L1111-8 CSP).
- Toute personne (visée par l'article précité) qui contreviendrait à son obligation de secret professionnel encourt une peine d'un an d'emprisonnement et de 15 000 € d'amende. (art. 226-13 CP).
- Le personnel des sous-traitants/partenaires qui seraient amenés à accéder à la plateforme sont également soumis au secret professionnel.

Les deux agréments d'Orange

Comparaison des deux agréments

Agréments	**Health Data Solutions infogérance** d'application (full managé)	**Health Data Solutions OS-managé**
Service fourni	• Service d'infogérance de l'application qui est fournie par le client • Service de gestion du système d'exploitation et des ressources du client (CPU, Ram, Stockage) • Services de gestion de l'infrastructure réseau et sécurité mutualisée	• Service d'authentification forte pour les accès du client • Service de gestion du système d'exploitation et des ressources du client (CPU, Ram, Stockage) • Service de gestion de l'infrastructure réseau et sécurité mutualisée
Composants de l'agrément	• Deux datacenters en région parisienne • Plateforme CES Santé Dual Site • Application fournie par le client avec un rapport des exigences de l'agrément dans le contrat client	• Mêmes datacenters • Même plateforme : CES Santé Dual Site • Application fournie ET exploitée par le client avec un report des exigences de l'agrément dans le contrat client
Contrat/Marché	Modèle de contrat qui exclut les accès du client sur la plateforme et les serveurs Le périmètre de prestation et de responsabilité d'Orange est global à l'ensemble de la plateforme avec toutes les couches jusqu'au management opérationnel de l'application	Modèle de contrat qui attribue au client le rôle d'exploitant des composants logiciels et applicatifs de sa plateforme. Le périmètre de prestation et de responsabilité d'Orange s'arrête au système d'exploitation inclus
Support	L1, L2, et L3 en France	Même chaîne de support, mêmes équipes

Agrément Health Data Solutions « full managé »

Agrément obtenu le 21 octobre 2010 pour l'hébergement de données de santé à caractère personnel via la solution « Health Data Solutions » (à l'époque sous le nom de « Flexible Computing Santé ») qui permet d'héberger et d'administrer les applications du client.
Orange Business Services fournit et gère :

- L'architecture et l'infrastructure (data center, serveurs, stockages, sécurité…) ;
- Les systèmes d'exploitation et les logiciels d'infrastructure au catalogue et leurs licences ;
- L'installation de l'applicatif fourni par le client ;
- Le « patch management » et le monitoring des systèmes d'exploitation, des logiciels d'infrastructure, de l'applicatif du client.

Le client délègue ainsi la gestion quotidienne de son applicatif et ne fournit que les évolutions et les mises à jour de celui-ci.

Agrément Health Data Solutions « Co/OS-managé »

Un dossier a été déposé le 18 décembre 2012 et l'agrément obtenu le 22 octobre 2013 pour 2 niveaux de services : « OS Managé » et « Logiciel d'infrastructure Managé ».
Orange Business Services fournit et gère :

- L'architecture et l'infrastructure (data center, serveurs, stockage, sécurité…) ;
- Les systèmes d'exploitation et, en option, des logiciels d'infrastructure au catalogue et leurs licences ;
- Via un sas sécurisé, les comptes des administrateurs du client, avec des droits nécessaires ;
- Le « patch management » et le monitoring des systèmes d'exploitation (en option également ceux des logiciels d'infrastructure).

Le client gère donc directement son application et les logiciels qu'il a lui-même installés.

Extension du périmètre de ces agréments : « l'accès patient »

Le 2 mars 2015, Orange Healthcare a obtenu du ministère de la Santé une extension de périmètre des 2 agréments pour la possibilité d'héberger des applications auxquelles le patient peut accéder directement.
Cet accord est soumis à la signature du client des nouveaux contrats mentionnant les obligations auxquelles il doit se conformer.
Ces obligations engagent le client sur la mise en œuvre d'une authentification forte et d'une identification sécurisée des patients.

Les exigences d'accès patient :

- Inscription préalable nécessaire :
  - Si l'inscription est faite par le professionnel de santé, il est responsable à la fois de l'identification formelle de la personne (carte vitale, carte d'identité...) et de la diffusion confidentielle des identifiants utilisés par les patients pour se connecter aux applications ;
  - Si l'inscription se fait en ligne par la personne concernée par les données hébergées, le processus d'inscription à l'application doit inclure les formulaires nécessaires à la capture de toutes les informations qui identifient de manière unique cette personne, qui seront reprises dans le processus d'authentification.
- Processus d'authentification forte intégrant plusieurs principes :
  - Le mot de passe à usage unique (OTP) ou équivalent (Grid) diffusé par mail ou SMS ;
  - Le double facteur : quelque chose que l'utilisateur sait (son compte) et quelque chose que l'utilisateur possède (téléphone mobile ou messagerie mail personnelle).

Cas spécifique du client éditeur

Seuls peuvent accéder aux données ayant fait l'objet d'un hébergement les personnes (que celles-ci concernent les professionnels de santé ou établissements de santé qui les prennent en charge étant désignés par les personnes concernées), selon des modalités fixées dans le contrat prévu au deuxième alinéa, dans le respect des dispositions des articles L. 1110-4 et L. 1111-7 (art. L1111-8 al. 7 CSP).
Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreintes au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal. (al. 10 art. L1111-8 CSP).
L'hébergeur ne peut transmettre les données de santé à caractère personnel à d'autres personnes que les professionnels de santé ou établissements de santé désignés dans le contrat de prestation d'hébergement (art. L1111-8 al. 8 CSP).

Exception de la procédure d'urgence

À titre exceptionnel, il est possible de permettre un accès temporaire de l'éditeur de logiciel à la plateforme d'hébergement de données de santé.
Cet accès doit être strictement encadré et rendu possible à condition de respecter les conditions suivantes :

- Niveaux d'habilitation fins pour savoir qui accède à la plateforme et quand (traçabilité des accès) ;
- Accès par le biais d'une authentification forte ;
- Limitation des accès à ce qui est strictement nécessaire ;
- Engagement de confidentialité de l'éditeur ;
- Accès sous le contrôle du médecin hébergeur et du RSSI pour encadrer les accès.

En route vers la certification

La règlementation autour de l'hébergement de données de santé évolue de l'agrément vers une certification. Celle-ci s'appuie sur des normes internationales, et s'inscrit dans la loi de 2016. Elle devra mettre en œuvre les normes ISO 20000, 27001 et 27018, avec un audit de surveillance annuel.
Orange Healthcare s'y prépare pour fin 2018. Merci de nous contacter pour plus d'information.