# CODE DE L'AFHADS

Mai 2018

Association Française des Hébergeurs Agréés de Données de Santé à caractère personnel

# CODE DE L'AFHADS

Adopté en assemblée générale du 26 octobre 2017

## Avant-propos

### Objet

Depuis 2009, l'agrément d'hébergeur de données de santé à caractère personnel atteste de la capacité de son titulaire à déployer des applications manipulant des données de santé à caractère personnel en garantissant un niveau minimum de contrôle par l'hébergeur de règles communes portant sur l'identification et l'authentification des utilisateurs, ainsi que la traçabilité des accès aux données hébergées.

Le référentiel de certification proposé par l'ASIP Santé pour remplacer cet agrément fait disparaitre ce rôle de contrôle. Il s'agit pour les hébergeurs de données de santé existants d'une régression, qui dévalorise leur offre alors même qu'elle bénéficiait d'une vraie reconnaissance de la part des acteurs et des citoyens, au point que des applications qui n'étaient pas formellement obligées de recourir à un hébergement agréé s'y soumettaient volontairement.

Le présent règlement vise à définir les conditions permettant à un hébergeur membre de l'AFHADS de délivrer des attestations de contrôle de conformité des applications et de les faire publier par l'AFHADS. Ces conditions comportent :

- Des règles de management portant sur l'organisation et les processus de l'hébergeur
- Un socle commun de prérequis pour le contrôle de conformité des applications

### Lien à la certification des hébergeurs

Une des dispositions du référentiel de certification (clause 24.9.2) impose à l'hébergeur de formaliser des prérequis à l'hébergement qui lui sont propres, de définir et d'appliquer une procédure de vérification de ces prérequis.

Les prérequis propres à l'hébergeur et la procédure de vérification associée devront être conformes au présent règlement pour permettre à un hébergeur de délivrer des attestations de contrôle de conformité.

En régime transitoire, les hébergeurs membres de l'association au titre d'un agrément antérieur à 2018 et toujours valide mais encore non certifiés sont également habilités à délivrer des attestations.

### Lien à la PGSSI-S

Les prérequis sont exprimés de la manière la plus large possible, afin de permettre l'extension de la marque HADS à des applications qui ne relèveraient pas de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

Lorsqu'ils sont applicables, les référentiels opposables de la PGSSI-S représentent toutefois la réalisation préférée des exigences. Si ce n'est pas le cas, les prérequis font appel à l'état de l'art, qui pourra être explicité dans des notes d'interprétation adjointes au présent code.

## Règles de management

Pour pouvoir délivrer des attestations de conformité, un hébergeur membre de l'AFHADS devra :

- Avoir inclus dans les prérequis de qualification de l'application tous les items du socle commun décrit ici.
- Effectuer cette qualification avant la première mise en production de l'application et au moins une fois tous les trois ans.
- Ne délivrer l'attestation qu'aux applications ayant effectivement passé avec succès la qualification sur l'ensemble des points du socle commun.
- Tenir un registre des applications qualifiées conforme à l'article 30, 2° du Règlement Général sur la Protection des Données, même si sa taille lui permettrait d'en être dispensé.
- Désigner un délégué à la protection des données personnelles
- Employer un médecin de l'hébergeur, garant des conditions éthiques de l'hébergement, contact privilégié des personnes concernées.

## Socle commun de prérequis

- L'application a fait l'objet d'une étude d'impact sur la vie privée.
- L'application est conforme à l'ensemble des exigences légales et réglementaires propres à la donnée de santé.
- Même en l'absence d'exigences réglementaires applicables, l'application est conforme à l'état de l'art, compte tenu du niveau de sensibilité des données manipulées, en termes d'identification des utilisateurs, de procédés d'authentification et d'imputabilité des accès.
- Les mesures mises en œuvre en matière d'identification, d'authentification et d'imputabilité sont documentées dans le registre tenu par l'hébergeur.
- L'application n'a présenté aucune vulnérabilité critique ou élevée au cours d'un test des attaques les plus courantes.

## Date de retrait de la version antérieure

Il n'y a pas de version antérieure à retirer.

Le code n'est applicable que dans le cadre d'une certification, les hébergeurs encore non certifiés et membres de l'association au titre d'un agrément en cours n'y sont pas soumis.

# ATTESTATION DE CONFORMITE

L'application <NOM D'APPLICATION> est hébergée par <ACME >, membre de l'Association Française des Hébergeurs Agréés de Données de Santé (AFHADS).

<ACME> a contrôlé le <Date> la conformité de l'application aux règles établies par l'AFHADS dans l'édition 2017 de son Code de Marque :

- L'application a fait l'objet d'une étude d'impact sur la vie privée.
- L'application respecte l'ensemble des exigences réglementaires propres à la donnée de santé.
- L'application est conforme à l'état de l'art, compte tenu du niveau de sensibilité des données manipulées, en termes d'identification des utilisateurs, de procédés d'authentification et d'imputabilité des accès.
- L'application a passé avec succès un test de vulnérabilité aux attaques courantes.

En conséquence de quoi, la marque de contrôle ci-dessous peut être apposée sur les écrans et la documentation de l'application.


*Détails de la version qualifiée*

*<A renseigner avec la version et les conditions spécifiques de mise en œuvre si elles sont nécessaires>*

Fait à <Lieu> le <Date>

Pour <ACME >

<Identité et rôle du signataire>

<Signature - Egalement signature numérique du PDF>