L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

# I. DANS QUEL CAS PARLE-T-ON D'HÉBERGEMENT DE DONNÉES DE SANTÉ ?


- Q1 : Qu'est-ce que la donnée de santé ?
- Q2 : Dans quelle situation parle-t-on d'hébergement de donnée de santé ?
- Q3 : Dois-je informer le patient ?
- Q4 : Quelles sont les activités soumises à la certification HDS ?


### CHAMP D'APPLICATION : PRÉCISIONS APPORTÉES PAR LE MINISTÈRE DE LA SANTÉ ET DES SOLIDARITÉS


- Q5 : Qui est concerné par l'hébergement de données de santé ?
- Q6 : Qui n'est pas concerné par l'hébergement de données de santé ? (exemples)


# II. COMMENT SE DÉROULE LA PROCÉDURE DE CERTIFICATION ?


- Q7 : Où peut-on trouver les différents documents liés aux processus d'accréditation et de certification HDS?


### JE SOUHAITE DEVENIR ORGANISME DE CERTIFICATION (OC)


- Q8 : Quelles sont les étapes du processus d'accréditation ?
- Q9 : Quelle est la durée de l'accréditation ?


### JE SUIS/SOUHAITE ÊTRE HÉBERGEUR DE DONNÉES DE SANTÉ (HDS)


- Q10 : Quelles sont les étapes du processus de certification ?
- Q11 : Comment certifier un hébergeur qui n'héberge pas encore de données de santé ?
- Q12 : Je suis un hébergeur candidat à la certification HDS. Mes sous-traitants doivent-ils être certifiés ?
- Q13 : Je dispose déjà d'une certification ISO 27001. Suis-je obligé de recourir au même organisme de certification que celui qui m'a délivré la certification ISO 27001 ?
- Q14 : J'ai déposé un dossier d'agrément, dois-je changer de procédure ?
- Q15 : Je suis hébergeur agréé HDS, mon agrément est-il toujours valide ?
- Q16 : Je suis un hébergeur certifié HDS (ou en cours de certification). Que se passe-t-il lorsque l'accréditation de mon organisme de certification est suspendue ?
- Q17 : Je suis un hébergeur certifié HDS. Mon organisme de certification perd son accréditation, que se passe-t-il ?

# I. DANS QUEL CAS PARLE-T-ON D'HÉBERGEMENT DE DONNÉES DE SANTÉ ?

## Q1 : Qu'est-ce que la donnée de santé ?

Le règlement européen sur la protection des données personnelles donne une définition depuis avril 2016. Ce sont les données relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.
Des précisions sont apportées sur le site de la CNIL.

## Q2 : Dans quelle situation parle-t-on d'hébergement de donnée de santé ?

L'article L.1111-8 du code de la santé publique indique que :
« 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 ou 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**, doit être agréée ou certifiée à cet effet ».

## Q3 : Dois-je informer le patient ?

L'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime. L'obligation d'information pèse sur l'hébergeur. Il lui appartient de déterminer les modalités de délivrance de cette information (par lui-même ou par ses clients) et de les formaliser dans le contrat HDS.

## Q4 : Quelles sont les activités soumises à la certification HDS ?

Les activités entrant dans le périmètre de l'hébergement de données de santé sur support numérique sont définies en distinguant deux catégories de métiers « hébergeur de données de santé » :

- **L'hébergeur d'infrastructure physique** pour les activités suivantes :
  - mise à disposition et maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
  - mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.
- **L'hébergeur infogéreur** pour les activités suivantes :
  - mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
  - mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
  - administration et exploitation du système d'information contenant les données de santé ;
  - sauvegarde externalisée de données de santé.

L'activité d'hébergement de données de santé à caractère personnel sur support numérique consiste à exercer pour le compte d'un tiers (responsable de traitement, patient, etc.) tout ou partie des activités listées ci-dessus.
L'hébergeur devra être certifié sur le périmètre des activités qu'il propose.

## Q5 : Qui est concerné par l'hébergement de données de santé ?

Le Ministère des Solidarités et de la Santé précise que **les personnes physiques ou morales** concernées par l'hébergement de données de santé sont d'une part, **les patients** qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part les **responsables de traitements de données de santé à caractère personnel** ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes.

## Q6 : Qui n'est pas concerné par l'hébergement de données de santé ? (exemples)

Le Ministère des Solidarités et de la Santé précise un certain nombre de situations qui ne sont pas concernées par l'hébergement de données de santé.
A titre d'exemple, sont exclues de l'obligation de recourir à un prestataire agréé ou certifié HDS : les organismes d'assurance maladie obligatoire ou complémentaire dans le cadre de leur activité de prise en charge des frais de santé, 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, etc.

# II. COMMENT SE DÉROULE LA PROCÉDURE DE CERTIFICATION ?

### Q7: Où peut-on trouver les différents documents liés aux processus d'accréditation et de certification HDS?

Le règlement d'accréditation, le dossier de candidature, ainsi que le document d'exigences spécifiques pour le schéma de certification HDS sont à disposition sur le site internet du Cofrac.
Les référentiels d'accréditation et de certification HDS dits « référentiels HDS » publiés au Journal Officiel sont disponibles sur le site de l'ASIP Santé.

## JE SOUHAITE DEVENIR ORGANISME DE CERTIFICATION (OC)

### Q8: Quelles sont les étapes du processus d'accréditation ?

Le schéma d'accréditation des OC HDS a ouvert le 15 juillet 2018.
Les modalités d'accréditation sont définies dans le référentiel d'accréditation HDS, et dans le document « exigences spécifiques pour l'accréditation des organismes procédant à la certification de systèmes de management dans le domaine des technologies de l'information » émis par le Cofrac.

En synthèse, les principales étapes de l'accréditation des organismes de certification sont les suivantes:

- L'organisme complète et envoie le dossier de candidature à l'accréditation HDS auprès du Cofrac ;
- Le Cofrac examine la complétude du dossier de candidature (phase de recevabilité administrative) et le cas échéant, conclut un contrat avec l'organisme ;
- Le Cofrac étudie le respect par l'organisme des exigences d'accréditation (phase de recevabilité technique). Cette phase dure en moyenne de 1 à 6 mois ;
- Dès que la recevabilité technique favorable de la demande d'accréditation est prononcée par le Cofrac, l'organisme est autorisé à délivrer des certificats HDS pendant 9 mois ;
- L'organisme de certification dispose d'un délai de neuf mois pour finaliser son accréditation, qui se matérialise par une évaluation au siège de l'organisme, et une observation d'audit sur site par le Cofrac.

### Q9: Quelle est la durée de l'accréditation ?

L'accréditation est délivrée pour une durée de 4 ans avec une évaluation siège, ainsi qu'une observation d'audit tous les 12 mois.
Pour les cycles suivants, l'accréditation est délivrée pour une durée de 5 ans avec une évaluation siège et une observation tous les 15 mois.

## JE SUIS/SOUHAITE ÊTRE HÉBERGEUR DE DONNÉES DE SANTÉ (HDS)

### Q10: Quelles sont les étapes du processus de certification ?

- L'hébergeur choisit un organisme certificateur accrédité par le Cofrac (ou autre instance nationale d'accréditation au niveau européen) ;
- L'organisme procède à un audit documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification ;
- L'organisme procède à un audit sur site du système dans les conditions définies dans le référentiel d'accréditation.

### Q11 : Comment certifier un hébergeur qui n'héberge pas encore de données de santé ?

Deux cas sont possibles :
**Cas 1** : L'hébergeur est en mesure de démontrer l'application de son système de management de la sécurité de l'information HDS (SMSI), pour l'hébergement d'autres types de données que celles visées dans le décret HDS.
La certification HDS est délivrée en évaluant le SMSI de l'hébergeur appliqué à l'hébergement de ces autres données.
**Cas 2** : L'hébergeur n'est pas en mesure de démontrer l'application de son système de management de la sécurité HD.
La certification HDS est délivrée après un audit restreint sur les éléments disponibles.
Les éléments non audités devront l'être dès que possible et au plus tard lors du premier audit de surveillance annuel.

### Q12: Je suis un hébergeur candidat à la certification HDS. Mes sous-traitants doivent-ils être certifiés ?

L'hébergeur de données de santé a le choix.

- L'hébergeur peut recourir à un sous-traitant non certifié s'il respecte les exigences relatives à la gestion des relations avec les fournisseurs prévues dans les normes. Le cas échéant, l'hébergeur doit, notamment :
  - prendre en compte les relations avec les fournisseurs dans sa politique de sécurité de l'information et intégrer des exigences de sécurité dans les contrats avec ses fournisseurs ;
  - mettre en place une surveillance et auditer ses fournisseurs.
- L'hébergeur peut recourir à un sous-traitant certifié. Ce sous-traitant doit :
  - être certifié sur un périmètre de certification qui recouvre le périmètre de la sous-traitance ;
  - avoir un certificat valide.

## Q13: Je dispose déjà d'une certification ISO 27001. Suis-je obligé de recourir au même organisme de certification que celui qui m'a délivré la certification ISO 27001 ?

Il n'y a pas d'obligation.
Pour obtenir la certification HDS, un hébergeur peut recourir au même organisme de certification qui lui a délivré sa certification ISO 27001, si ce dernier est accrédité HDS ou à un autre organisme de certification accrédité HDS.

Pour se prévaloir d'une certification ISO 27 001 déjà obtenue, la certification doit respecter les conditions d'équivalence du certificat précisées au point 7.2 du référentiel d'accréditation HDS et notamment celle relative au périmètre d'application de la certification déjà obtenue : cette dernière doit inclure le périmètre pour lequel le candidat demande une certification HDS.

## Q14: J'ai déposé un dossier d'agrément, dois-je changer de procédure ?

Les demandes d'agrément et de renouvellement d'agrément déposées avant le 31 mars 2018 sont instruites selon la procédure d'agrément pour l'hébergement de données de santé sur support électronique (décret n°2006-6 du 4 janvier 2006). Les agréments délivrés sont valables trois ans.

## Q15 : Je suis hébergeur agréé HDS, mon agrément est-il toujours valide ?

Les agréments produisent leur effet jusqu'à leur terme. L'entrée en vigueur de la procédure de certification n'a pas d'incidence sur les agréments.
Lorsque l'agrément arrive à échéance avant le 31 mars 2019, la durée de l'agrément est prolongée pour une durée de six mois afin de permettre à l'hébergeur d'effectuer les démarches de certification nécessaires à la poursuite de son activité d'hébergement de données de santé.
Pour poursuivre son activité HDS, l'hébergeur doit au plus tard, à la date d'échéance de son agrément, être certifié HDS.

## Q16: Je suis un hébergeur certifié HDS (ou en cours de certification). Que se passe-t-il lorsque l'accréditation de mon organisme de certification est suspendue ?

La décision de suspension de l'accréditation est notifiée à l'organisme de certification par le Cofrac (ou équivalent au niveau européen).
La décision de suspension précise :

- la portée de la suspension de l'accréditation ;
- les motivations de la décision de suspension ;
- les conditions de levée de la suspension.

L'organisme de certification doit en informer ses clients hébergeurs (déjà certifiés ou en cours de certification) et cesser ses activités de certification HDS pendant la durée de la suspension. Pendant la période de suspension, il ne peut pas réaliser d'audit ni rendre de décisions relatives à la certification HDS.
Nota bene : pendant la période de suspension, les certificats HDS déjà délivrés par l'organisme certificateur restent valides.

## Q17: Je suis un hébergeur certifié HDS. Mon organisme de certification perd son accréditation, que se passe-t-il ?

Le Cofrac notifie le retrait d'accréditation à l'organisme de certification et à l'ASIP Santé. L'organisme de certification doit en informer ses clients hébergeurs afin que ces derniers transfèrentleur certification à un autre organisme de certification.

L'ASIP Santé tient à jour la liste des OC accrédités qui lui est transmise par le COFRAC.

NB : un retrait d'accréditation est prononcé à la suite d'une suspension.