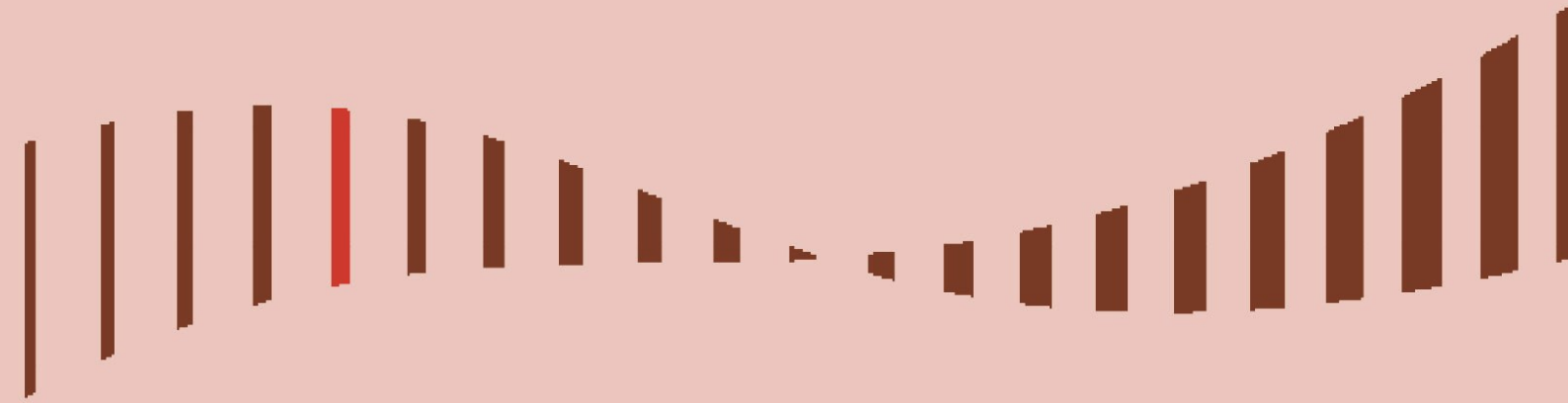
VERSION
0.3.0

Référentiel de certification HDS
Vue d'ensemble

Septembre 2016 - V0.3.0



asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Sommaire

Avant-propos

Le présent document a pour objet de présenter les modifications de la procédure d'agrément pour l'hébergement de données de santé proposés par l'article 204-I-5)-c) de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, qui prévoit de la remplacer par une procédure de certification.

Les exigences et éléments retenus dans le cadre de cette nouvelle procédure découlent des obligations définies à l'article L.1111-8 du code de la santé publique et s'inspirent de ceux prévus aux articles R.1111-9 et suivants du code de la santé publique relatifs à l'actuelle procédure d'agrément pour l'hébergement des données de santé.

Les objectifs poursuivis par la nouvelle procédure de certification sont d'inscrire la démarche dans une procédure bien connue du monde industriel et d'accroître la fiabilité du contrôle des exigences par des audits sur site. Pour ce faire, la démarche conduit à mettre en place une certification des entreprises offreuses de services d'hébergement de données de santé (celle-ci étant cependant distinguée en deux niveaux : fourniture d'environnement d'hébergement seul ou environnement d'hébergement et exploitation de la couche applicative). Le choix des normes retenues pour la nouvelle procédure a été approuvé par l'ensemble des fédérations d'industriels.

Cette certification aura un caractère plus générique sur la base des seules responsabilités de l'hébergeur, celles-ci étant clairement distinguées de celles du responsable de traitement (ses responsabilités étant identiques qu'il héberge lui-même ses applications ou qu'il ait recours à un hébergeur).

Il résulte de ce choix que le respect par l'application mise en œuvre des principes de la PGSSI-S ne sera plus réalisé à l'occasion de la procédure de certification retirant à l'hébergeur qui portait le dossier devant la commission, la légitimité de relayer ces exigences vis-à-vis de son client. Cette clarification est soutenue par la majorité des fédérations d'industriels.

1.Introduction

Ce document s'adresse à l'ensemble des acteurs intéressés par l'hébergement de données de santé à caractère personnel (hébergeur éventuellement déjà agréé « hébergeur de données de santé », responsable de traitement de données de santé, organisme de certification souhaitant être accrédité pour certifier des hébergeurs, autorité compétente, et plus largement toute personne souhaitant avoir une vue d'ensemble des processus de certification pour l'hébergement de données de santé.

1.1. Contexte

1.1.1. Rappel du dispositif actuel d'agrément

La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a défini une nouvelle sphère de protection des données de santé en encadrant leur condition d'hébergement.

L'article L 1111-8 du code de la santé publique dispose ainsi que « *Toute personne 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 desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime*. »

Les conditions d'hébergement de données de santé à caractère personnel sur support informatique et la procédure d'agrément des hébergeurs, ont été précisées par le décret 2006-6 du 4 janvier 2006 (codifié aux articles R 1111-9 à R 1111-15-1 du code de la santé publique).

Conformément à l'article L 1111-8 du code de la santé publique et au décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel, toute personne physique ou morale hébergeant des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi pour le compte d'un tiers, doit être agréée par décision du ministre chargé de la santé qui se prononce après avis de la CNIL et d'un comité d'agrément des hébergeurs (organe consultatif crée par le décret 2006-6 précité). L'agrément est délivré pour une durée de trois ans. Si l'hébergeur agréé souhaite poursuivre son activité d'hébergement de données de santé au-delà des trois ans initiaux, il doit effectuer une demande de renouvellement d'agrément qui est instruite en suivant la même procédure que la demande initiale

Le Secrétaire Général du ministère chargé des affaires sociales a confié à l'ASIP Santé la gestion du secrétariat du comité d'agrément et la pré-instruction des dossiers de demande d'agrément pour le compte du comité d'agrément. Pour mener à bien cette mission, un comité d'instruction interne à l'ASIP Santé a été mis en place. Ce comité d'instruction pré-instruit les dossiers de demande d'agrément sous trois volets : « Sécurité & Technique », «Ethique & Juridique » et « Economique & Financier », tous trois fondés sur un référentiel élaboré en concertation avec la CNIL, les industriels et les maîtrises d'ouvrage régionales du secteur de la santé qui retranscrit les obligations définies par les articles L.1111-8 et R.1111-9 et suivants du code de la santé publique.

Depuis la publication du référentiel relatif à la composition des dossiers de demande d'agrément en 2009 et jusqu'à début 2016, le Comité d'agrément a reçu près de 300 dossiers et près de 100 décisions d'agréments ont été émises. L'écart entre ces deux chiffres comprend les dossiers en cours d'analyse, les dossiers retirés, les refus d'agrément et les dossiers de renouvellement.

1.1.2. Constat après cinq ans de fonctionnement

La présente procédure d'agrément a fait émerger des offres d'hébergement de données de santé dans des conditions de protection respectant la loi du 4 mars 2002 précitée. Elle a aussi permis la mise en conformité d'un certain nombre de services d'hébergement de données de santé pré existants.

Toutefois, la majorité des données de santé à caractère personnel reste probablement encore hébergée par des tiers hors du cadre juridique de l'agrément.

Les dossiers de demande sont déclaratifs (instruction uniquement sur pièces) et nécessitent une analyse approfondie qui entraîne une charge de traitement de 20 jours en moyenne, dont les deux tiers correspondent à l'instruction des dossiers (CNIL, CAH, ASIP Santé, Ministère de la santé) le tiers restant étant associé au traitement administratif du dossier par le secrétariat du CAH et à la gestion des relations avec les candidats. Le délai de traitement moyen est de six mois (le délai maximum prévu par les textes est de 8 mois). Mais dans 30% des cas, lorsque des compléments d'information sont demandés aux candidats, le délai d'instruction peut dépasser les huit mois prévus. L'évolution du nombre de dépôts de dossier étant peu prévisible, la réservation des ressources nécessaires à l'instruction est difficile.

Le référentiel d'agrément identifie des buts à atteindre par les hébergeurs et non les moyens à mettre en œuvre. Les candidats à l'agrément constituent donc leur dossier sans grille d'analyse leur permettant de s'assurer si les mesures de sécurité qu'ils prévoient sont nécessaires et suffisantes et sans pouvoir réellement évaluer leur capacité à être agréés.

Sur les conditions réelles d'hébergement, l'absence de mise en place de contrôles[1] et d'obligations d'audits externes par des auditeurs qualifiés empêche les pouvoirs publics d'avoir une vision concrète des réalités du terrain.

En outre, les textes relatifs à l'hébergement de données de santé et le référentiel d'agrément ne répondent pas toujours à l'évolution des conditions techniques et de l'offre commerciale des services d'hébergement.

Il est donc apparu nécessaire au législateur de proposer une adaptation des conditions d'hébergement de données de santé, avec pour finalité principale la protection des données de santé à caractère personnel.

Ainsi, pour répondre à ces limites, la loi de modernisation de notre système de santé précitée qui habilite le Gouvernement à agir par voie d'ordonnance - *dans un délai de douze mois suivant la promulgation de la loi* – pour prendre *les mesures visant à simplifier la législation en matière de traitement des données personnelles de santé et visant à « remplacer l'agrément prévu au même article L. 1111-8 par une évaluation de conformité technique réalisée par un organisme certificateur accrédité par l'instance nationale d'accréditation mentionnée à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie ou par l'organisme compétent d'un autre État membre de l'Union européenne. Cette certification de conformité porte notamment sur le contrôle des procédures, de l'organisation et des moyens matériels et humains ainsi que sur les modalités de qualification des applications hébergées »*.

L'ordonnance précitée sera précisée par un décret qui définira la procédure de certification des hébergeurs de données de santé.

[1] La possibilité de contrôle par l'inspection générale des affaires sociales permise par les textes n'a jamais été mise en œuvre

1.2. Généralités

Ce document présente les grandes orientations du projet de référentiel de certification des hébergeurs de données de santé (HDS) et s'appuie sur le corpus documentaire suivant :

- le référentiel de certification « ASIP Santé - Exigences et contrôles du référentiel HDS » qui détaille les modalités de certification au référentiel HDS ;
- le référentiel d'accréditation « ASIP Santé - Accréditation des organismes de certification HDS » décrit les modalités permettant d'accréditer des organismes de certification ;
- la description de la gouvernance « ASIP Santé - Gouvernance du référentiel HDS » traite du maintien dans le temps du référentiel.

Il est organisé en quatre parties :

1. une introduction qui rappelle les grands principes de l'actuelle procédure d'agrément des hébergeurs de données de santé ;

2. une présentation du champ d'application de l'article L.1111-8 et des activités et services couverts par le référentiel de certification HDS ;

3. une présentation générale du référentiel de certification HDS, du référentiel d'accréditation et de la gouvernance ;

   cette partie s'adresse plus particulièrement aux hébergeurs de données de santé, aux chefs de projets travaillant sur des projets d'agrément ainsi qu'aux autorités compétentes impliquées dans l'une des procédures décrites dans l'un des documents du corpus documentaire ;

4. une annexe décrivant les activités et métiers d'hébergeur.

2.Champ d'application

L'article 96 de la loi de modernisation de notre système de santé a modifié la rédaction l'article L.1111-8 du code de la santé publique afin d'étendre son champ d'application organique.

Ainsi, toute personne physique ou morale qui met à disposition de tout responsable de traitement de données de santé un service d'hébergement de données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social a l'obligation d'être agréée pour l'hébergement de données de santé. Avant la mise en œuvre de la procédure de certification, un décret va venir préciser le champ d'application du nouvel article L.1111-8 (définition de la notion d'hébergement, catégories d'acteurs concernés, etc.)

L'obligation d'agrément sera remplacée par une obligation de certification.

Par conséquent, « demain » toute personne physique ou morale qui mettra à disposition de tout responsable de traitement de données de santé, un service d'hébergement de données de santé à caractère personnel aura l'obligation d'être certifiée pour l'hébergement de données de santé.

Les modalités de certification seront précisées par un décret en Conseil d'Etat qui renverra la définition des exigences techniques au référentiel de certification présenté ci-dessous.

Deux types de certification[2] sont définis dans le référentiel :

- une certification « hébergeur d'infrastructure » pour les activités d'hébergement physique, de mise en œuvre de matériels informatiques et de maintenance de matériels informatiques ;
- une certification « hébergeur infogérant » pour les activités d'hébergement physique mais aussi l'activité d'infogérance et de sauvegardes externalisées.

Les activités ci-dessus sont définies dans le chapitre 4 du présent document

Dans la suite du document, le terme certification utilisé seul peut désigner indifféremment l'une ou l'autre de ces certifications HDS.

[2] Les dénominations de deux types de certifications restent à définir.

3.Vue d'ensemble du référentiel HDS

3.1. Référentiel de certification : exigences et contrôles du référentiel

Le référentiel de certification présente les modalités de certification des hébergeurs de données de santé.

Il décrit :

- les exigences du référentiel auxquelles doivent répondre les candidats ;
- le cycle de vie du certificat HDS (durée, conditions d'audit de surveillance, durée de validité du certificat, sanctions éventuelles) ;
- les modalités de contrôles.

Un candidat souhaitant obtenir une certification devra répondre aux exigences du référentiel et faire une demande de certification auprès d'un organisme de certification (OC) accrédité par le COFRAC (ou équivalent au niveau européen).

Pour obtenir une certification, un hébergeur devra

- exploiter un système de gestion de la sécurité des informations conforme à la norme ISO/CEI 27001:2013 sur le périmètre du système de gestion de la sécurité des informations pour le métier « hébergeur d'infrastructure » ou le métier « hébergeur infogérant ». ;
- être évalué pour la conformité vis-à-vis
    - d'exigences relatives à la protection des données à caractère personnelles qui s'appuient sur l'ISO 27018:2014 ;
    - d'exigences relatives à la gestion des services qui s'appuient sur l'ISO 20000:2011 ;
    - d'exigences spécifiques au domaine de la santé.

La certification ISO 27001:2013 est obligatoire pour être certifié HDS.

Les certifications ISO 27018:2014 et ISO 20000:2011 ne sont pas exigées et seules des exigences extraites de ces certifications doivent être respectées par l'hébergeur.

Un hébergeur disposant déjà d'une certification ISO 27001:2013 ou ISO 2000 :2011 ne sera évalué que sur le périmètre des exigences non couvertes par ses certifications[3].

La certification ISO 27018:2014 étant émise hors accréditation, la notion d'équivalence ne s'applique pas à cette norme.

Les chapitres suivants décrivent brièvement les processus standards de certification, de suspension et de retrait d'un certificat, qui pourront sur certains points faire l'objet d'aménagements s'agissant de la certification HDS. La description détaillée des activités composant ces processus se trouve dans le document « exigences et contrôles du référentiel ».

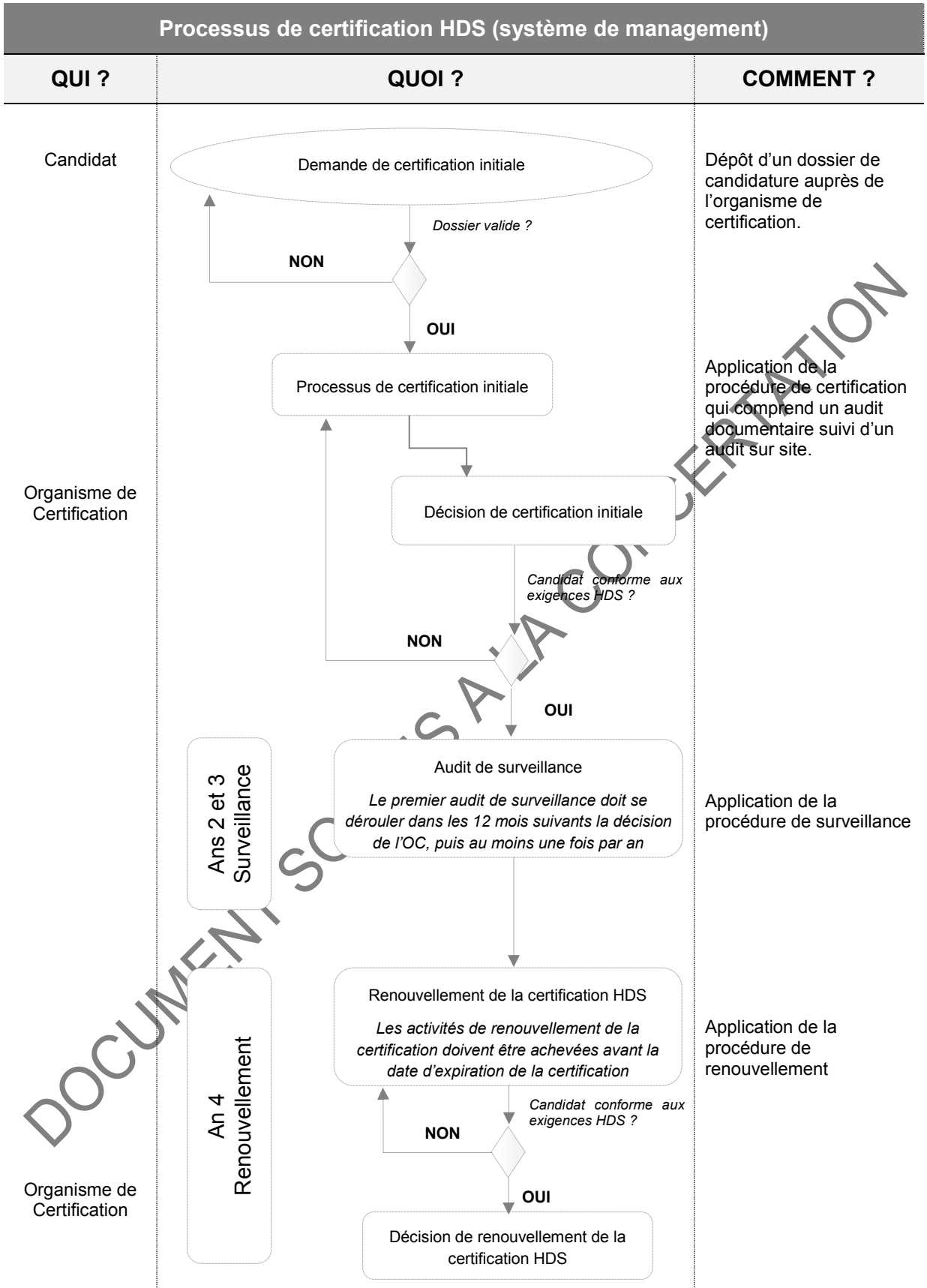
Une étude juridique est en cours pour les adapter à la certification HDS.

3.1.1. Processus de certification

Le processus de certification HDS est représenté dans le schéma suivant. Il se base sur le processus standard de type système de management (cf. ISO/CEI 17021).

Les coûts de certification sont à la charge de l'hébergeur.

[3] Après vérification de la validité et de la pertinence de la certification déjà obtenue par l'hébergeur par l'organisme de certification.



3.1.2. Processus de suspension du certificat

Ce chapitre décrit un processus de suspension conforme aux standards. Une étude juridique est en cours afin de l'adapter à la certification HDS.

Un certificat peut faire l'objet d'une suspension de 3 mois pouvant être reconduite une fois.

La suspension peut intervenir notamment en cas d'écarts constatés par rapport aux exigences du référentiel de certification HDS ou de non-respect des dispositions définies dans la procédure de surveillance.

3.1.2.1. Suspension à l'origine de l'organisme de certification

L'organisme de certification doit mettre en œuvre une activité de surveillance afin d'assurer un suivi régulier des certifications qu'il a délivrées. Cette activité de surveillance doit comporter des audits sur site permettant de vérifier la conformité du système de management de l'hébergeur certifié.

En cas d'écart constaté, l'organisme de certification doit suspendre un certificat, ce dernier doit communiquer par écrit au client sa décision de suspension suite à l'observation d'un manquement listé ci-dessus. La lettre devra détailler :

- La décision de suspension en décrivant les constats de la situation, les arguments ainsi que les références aux preuves objectives à l'origine de la suspension ;
- Le droit de réponse et d'appel à la décision. Dans le cas d'une suspension, l'hébergeur là 10 jours pour présenter par écrit une réponse ou un appel ;
- La date d'entrée en vigueur de la suspension correspondant à la date effective de réception de la lettre ;
- Les conditions et délais permettant à l'hébergeur de mettre un terme à la suspension, et les conséquences potentielles si des actions adéquates ne sont mises en œuvre ;
- Les moyens mis en œuvre par l'organisme de certification lui permettant de vérifier que les conditions sont à nouveau satisfaites et les actions correctives requises appliquées ;
- Une déclaration indiquant que le certificat est invalide pendant la période de suspension et que l'hébergeur doit cesser de se prévaloir de sa certification et supprimer toute communication relative à la certification.
- Une note mentionnant que l'hébergeur doit informer tout demandeur de la suspension du certificat.

Suite à la communication de la lettre, l'hébergeur peut faire appel de la décision de l'organisme de certification. Les appels sont traités, en premier niveau, par l'équipe d'audit ayant procédé à la certification de l'hébergeur, puis en deuxième niveau, par la direction générale avec consultation du comité d'impartialité de l'organisme de certification. L'appelant recevra, par la suite, un accusé de réception de son appel et sera tenu informé du traitement effectif de l'appel jusqu'en fin de processus.

La certification peut être réactivée sur la base de justification documentaire ou après un audit satisfaisant.

En cas d'échec, la certification sera retirée et le contrat annulé. L'organisme aura l'obligation de cesser toute publicité sur son ancienne certification et devra appliquer le processus de retrait.

3.1.3. Processus de retrait du certificat

Ce chapitre décrit un processus de retrait conforme aux standards pour la gestion des certifications. Il sera complété afin de prendre en compte les conclusions des travaux juridiques.

La certification d'un hébergeur peut faire l'objet d'un retrait sur décision de l'organisme certificateur suite au constat :

- d'une cessation d'activité définitive de l'hébergeur ;
- d'un non-respect répété des exigences définies dans le référentiel de certification ;
- d'écarts répétés par rapport aux exigences du référentiel de certification;
- du non-respect des dispositions des délais de la période de surveillance définie précédemment ;
- d'une pratique frauduleuse de l'activité d'hébergeur du non-exercice d'activité concernant le certificat d'hébergeur de données de santé délivrée, et ce pendant une période de plus d'un an.

À la suite du retrait du certificat, l'hébergeur doit cesser de se prévaloir de sa certification et supprimer toute communication relative à la certification faisant l'objet du retrait. De plus, à date de réception de l'écrit de l'organisme de certification, l'hébergeur doit informer l'ensemble de ses clients de la décision de retrait du certificat.

3.2. Accréditation des organismes de certification

[Cette partie fera l'objet d'une mise à jour à l'issue de travaux prévus avec le COFRAC]

La procédure d'accréditation s'applique aux organismes de certification responsables de l'activité d'évaluation des hébergeurs de données de santé à caractère personnel.

Les organismes de certification des hébergeurs de données de santé devront être accrédités par le COFRAC (Comité français d'accréditation) en France ou ses homologues européens. Cette accréditation est une attestation de compétence pour réaliser des contrôles, telle que définie à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.

La finalité et les modalités d'accréditation des organismes de certification sont définies dans le référentiel d'accréditation : :

- les conditions et critères que doit satisfaire un organisme de certification pour certifier des hébergeurs de données de santé à caractère personnel ;
- les modalités d'évaluation permettant à l'autorité compétente d'accréditer les organismes de certification ;
- les responsabilités des organismes certificateurs.

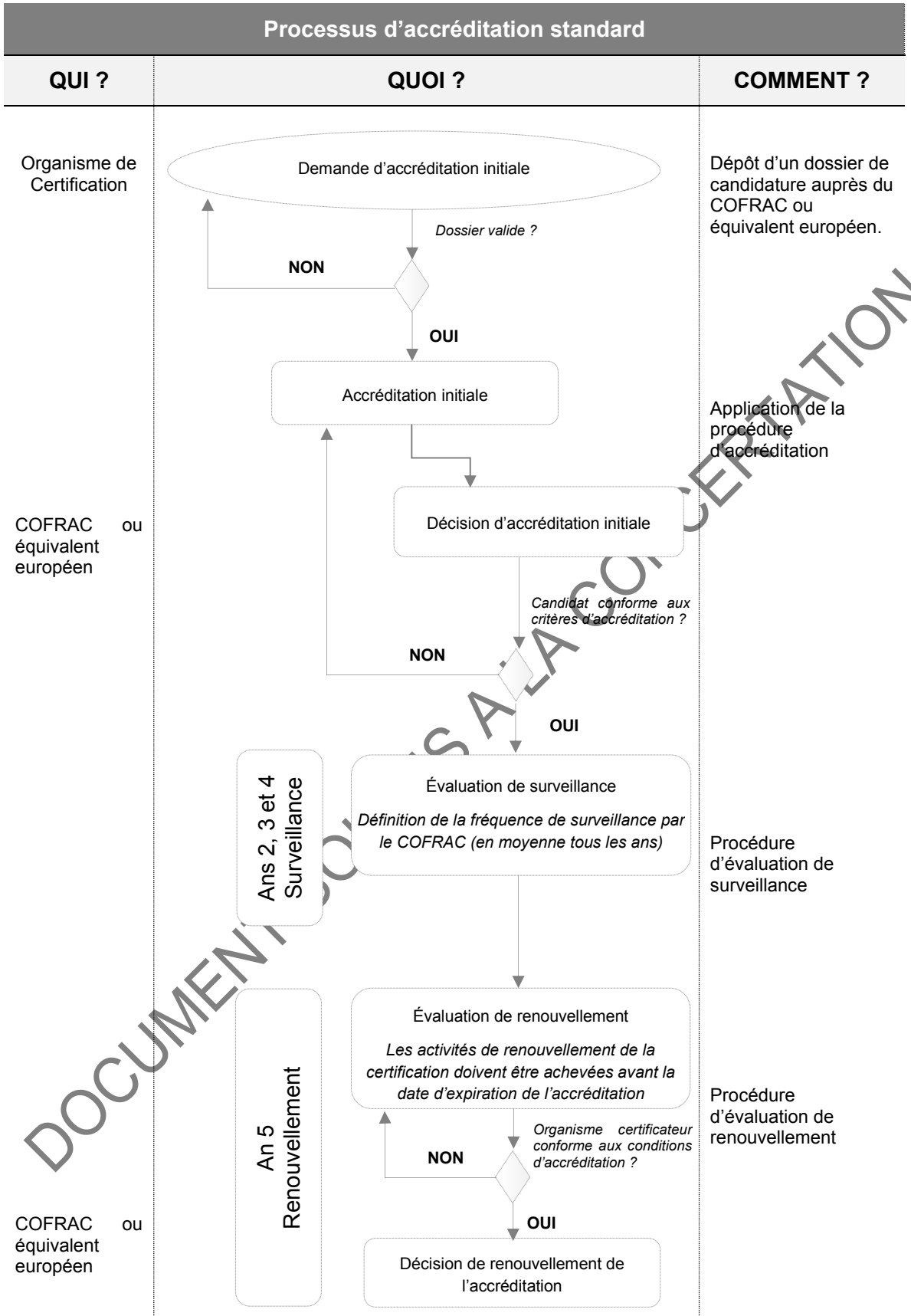
Le document définit ainsi la démarche d'accréditation dans le contexte d'hébergement de données de santé et l'organisation permettant de garantir l'harmonisation des pratiques relatives aux métiers d'hébergeur pour instaurer une confiance dans les prestations réalisées.

Les modalités d'accréditation s'inspirent et reprennent des exigences de la norme ISO/CEI 27006:2015.

Le référentiel d'accréditation proposé doit faire l'objet de travaux avec le COFRAC et de travaux juridiques, notamment s'agissant des éléments relatifs à la suspension et au retrait d'une accréditation.

3.2.1. Processus d'accréditation standard

Le schéma suivant représente le processus standard (ISO/CEI 27006:2015) d'une accréditation. Différents éléments devront être ajustés suite aux travaux prévus avec le COFRAC.



Remarque : Le déroulement du processus d'accréditation décrit ci-dessus ne détaille pas les différentes étapes composant la procédure. Se référer au document relatif à l'accréditation du référentiel afin d'avoir une vision exhaustive des différentes étapes.

3.2.2. Processus de suspension de l'accréditation

3.2.2.1. Décision de suspension

Dans le cas d'une suspension, l'organisme d'accréditation informe sans délai l'organisme certificateur, de toute mesure de suspension ou de retrait d'accréditation ou de toute annonce de cessation d'activité.

La décision de suspension est notifiée par lettre recommandée avec accusé de réception et précise la portée de la suspension de l'accréditation, les motivations de la décision de suspension de l'organisme d'accréditation ainsi que les conditions dans lesquelles l'organisme pourra récupérer son accréditation.

Si l'organisme certificateur ne soumet pas les réponses demandées par l'organisme d'accréditation dans les délais impartis spécifiés dans la décision de suspension, l'accréditation est retirée pour les activités de certification d'hébergeur de données de santé à caractère personnel.

Lors de la suspension de l'accréditation, l'organisme certificateur a l'obligation d'informer ses clients et cesser toute référence à l'accréditation. Un organisme dont l'accréditation est suspendue ne doit réaliser aucun audit de certification, ni rendre de décisions relatives au certificat d'hébergeur de donnée de santé.

Afin de se prémunir de tout risque de poursuite d'activité de certification par un organisme suspendu, le COFRAC a la possibilité d'intervenir sur site afin de s'assurer que les activités ont été réalisées avant la prise d'effet de la suspension.

3.2.2.1. Levée de suspension

Dans les cas de suspension non volontaires, les conditions de levée de la suspension sont spécifiées dans la décision de suspension communiquée à l'organisme certificateur.

Dans les cas de suspension volontaires, la décision de levée de suspension est obligatoirement prise suite à une évaluation sur site ou de l'examen d'un rapport d'audit interne transmis par l'organisme certificateur au COFRAC. Si le rapport ne fournit pas d'éléments suffisants pour démontrer la conformité aux exigences d'accréditation, l'organisme certificateur est informé par courrier que sa suspension ne pourra être levée qu'au vu des résultats d'une évaluation sur site. Il a la possibilité de faire appel de la décision de refus de levée de suspension.

La décision de levée de suspension est notifiée par le COFRAC. Une nouvelle attestation d'accréditation mentionnant la date de prise d'effet de la levée de suspension est établie et l'annexe technique définissant les activités pour lesquelles l'accréditation a été accordée est mise à jour. La date de fin de validité de l'accréditation est inchangée.

Si le cycle d'accréditation est arrivé à échéance, l'organisme d'accréditation notifie un renouvellement d'accréditation. La nouvelle date de fin de validité de l'accréditation est déterminée en ajoutant 5 ans à la date de fin de validité associée au cycle d'accréditation précédent.

Que la suspension soit volontaire ou pas, l'accréditation ne peut être recouvrée qu'après soumission et examen des éléments permettant de vérifier la correction des non-conformités aux exigences d'accréditation pour les activités de certification d'hébergeur de données de santé, notifiée par écrit à l'organisme d'accréditation.

3.2.3. Processus de retrait de l'accréditation

Le retrait de l'accréditation prend effet à la date de notification du retrait par l'organisme d'accréditation. La décision est communiquée à l'organisme certificateur par lettre recommandée avec accusé de réception, précisant les motivations de la décision.

L'organisme certificateur dont l'accréditation a été retirée doit cesser toutes les activités liées à la certification d'hébergeur de données de santé et en informer immédiatement ses clients.

Dans le but de se prémunir de risque de poursuite d'activité non légitime de la part de l'organisme certificateur, l'organisme d'accréditation a la possibilité d'intervenir sur site afin de s'assurer que les activités ont été réalisées avant la prise d'effet de la suspension.

3.3. Gouvernance du référentiel

Le dernier document composant le corpus du référentiel HDS est relatif à la gouvernance du référentiel. Ce document a pour objectif de décrire les différentes étapes du processus de mise à jour du référentiel d'hébergeur de données de santé à caractère personnel et les règles de transition entre les versions du référentiel HDS.

3.3.1. Règles de transition entre l'agrément et la certification

Ce point sera défini dans la réglementation.

3.3.2. Règles de transition entre deux versions de référentiel de certification

Ce chapitre rappelle les principes de transition standard pour les systèmes de management.

3.3.2.1. Organismes de certification

Les organismes de certification accrédités par rapport à la version précédente du référentiel doivent analyser et évaluer l'impact des écarts entre les versions du référentiel HDS. Ils doivent établir un plan de transition pour déterminer à la fois les changements à leur système de gestion et le délai requis pour les exécuter afin de se conformer au nouveau référentiel HDS.

L'organisme de certification doit obtenir une validation du plan de transition auprès d'un organisme d'accréditation.

L'examen du plan permet à l'organisme d'accréditation d'identifier les points du référentiel HDS qui ont été interprétés différemment par l'organisme de certification et qui peuvent éventuellement conduire à des recommandations.

Cet examen devrait également permettre à l'organisme d'accréditation et à l'organisme de certification de se mettre d'accord sur une date de fin du processus de transition.

L'organisme de certification dispose de 2 ans pour obtenir une validation du plan de transition.

3.3.2.2. Hébergeurs de données de santé à caractère personnel

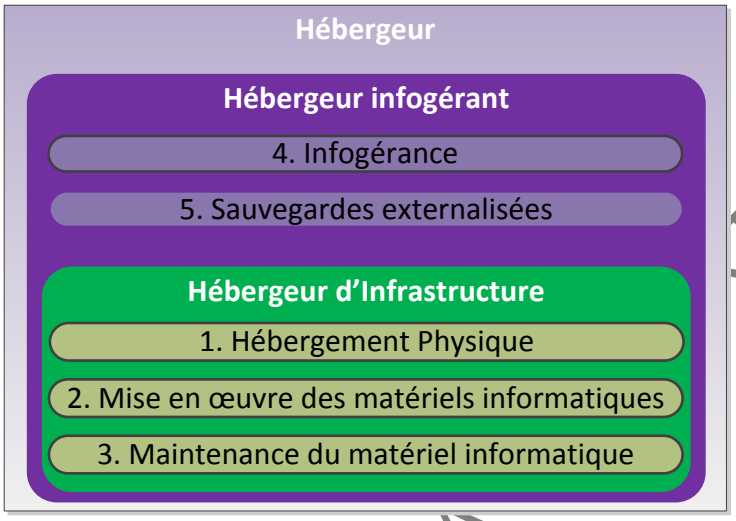
Lorsqu'une nouvelle version est publiée, les nouveaux candidats souhaitant être certifiés hébergeurs de données de santé pourront être certifiés selon la version précédente du référentiel pendant une période de deux ans. Au-delà de cette période, la certification se fera uniquement sur la base de la nouvelle version du référentiel.

En parallèle, les hébergeurs certifiés par rapport à la version précédente auront la possibilité d'exercer leurs activités d'hébergement de données de santé jusqu'à échéance de leur certificat.

Avant la date d'échéance du certificat, l'hébergeur devra se conformer aux exigences de la nouvelle version à travers la procédure de renouvellement qui s'appuie sur le nouveau référentiel.

4.Annexe : Activités

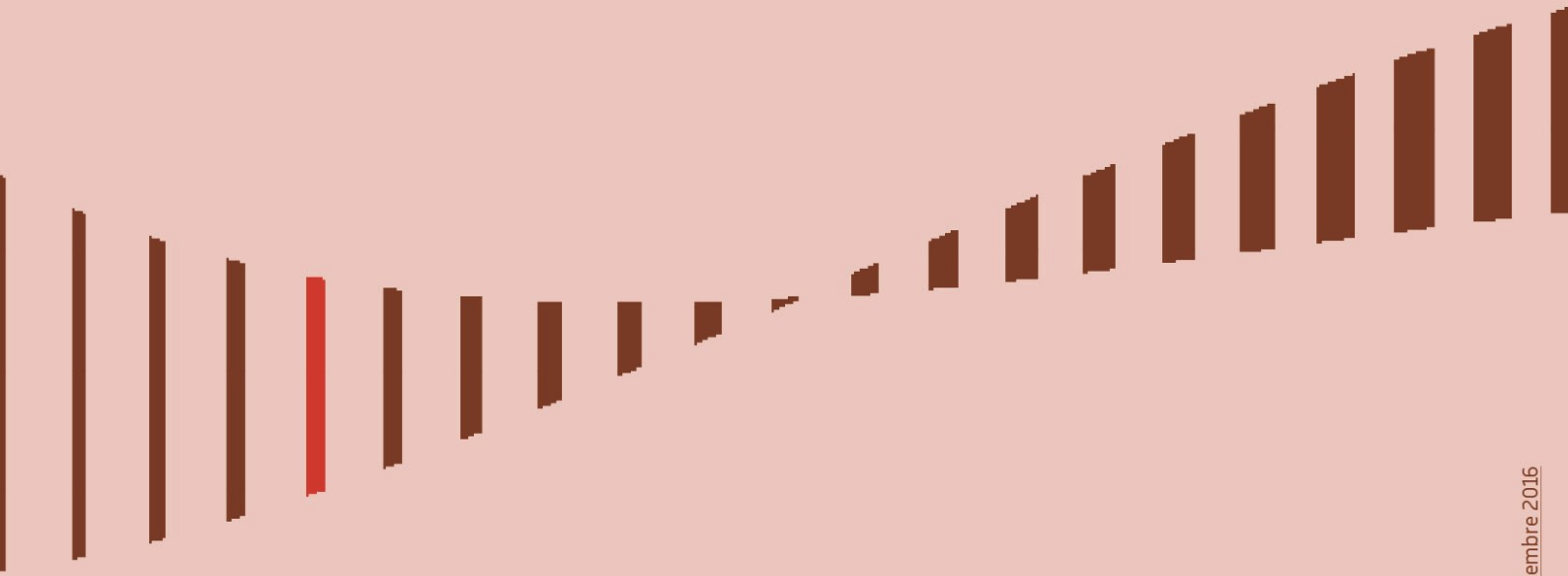
L'étude du marché de l'hébergement de données de santé montre que celui-ci est réalisé par un ensemble d'acteurs avec une répartition de responsabilités selon le périmètre d'intervention de chacun de ces acteurs.



Cette étude permet d'identifier cinq grandes familles d'activité dans le fonctionnement d'une application informatique potentiellement déléguées à un hébergeur :

1. Hébergement physique
   - Il s'agit de la fourniture des locaux ainsi que des services associés : climatisation, électricité et sécurité physique (intrusion, incendie, inondation).
   - Selon le niveau de qualité du service offert, l'alimentation électrique peut être redondante, il en est de même des accès aux opérateurs réseau (FAI) qui peuvent être doublés.
   - Ces services incluent en général une journalisation des accès sur le lieu et des interventions des prestataires externes (entretien, ménage, plomberie, électricité, etc.).
2. Mise en œuvre optionnelle des matériels informatiques
   - Il s'agit de la fourniture (initiale) des matériels informatiques (serveurs, moyens de stockage, etc.)
   - et du réseau (routeurs, firewall, multiplexeur, outil de gestion du trafic, etc.)
3. Maintenance optionnelle du matériel informatique (hardware)
   - Il s'agit de l'entretien et du dépannage du matériel informatique (serveurs, moyens de stockage, routeurs, firewall, etc.).
   - Ces prestations sont en général assurés par des tiers et non les fabricants de matériel eux-mêmes.
   - L'attention est attirée sur la nécessité de gérer la confidentialité des données enregistrées sur les supports physiques (ex : disques) remplacés.

4. Infogérance
    - Il s'agit de mettre en œuvre et maintenir en fonctionnement informatique le réseau, les serveurs, les machines virtuelles, les bases de données et les applications. Ceci couvre les fonctions suivantes :
        - système d'exploitation, middleware, logiciel métier,
        - administration quotidienne,
        - supervision,
        - installation des composants nécessaires au bon fonctionnement du système, des patchs, des nouvelles versions (niveau middleware et système),
        - gestion des tiers (intervenant sur l'environnement matériel ou logiciel),
        - gestion de la capacité.
5. Sauvegardes externalisées
    - Dans certains cas, les sauvegardes peuvent être stockées dans un site différent du site informatique.



L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Agence des Systèmes d'Information Partagés de Santé
9, rue Georges Pitard
Standard : 01 58 45 32 50
Du lundi au vendredi (hors jours fériés)
de 8h30 à 13h et de 14h à 17h
esante.gouv.fr