Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

Arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

NOR : *SSAZ1807891A*

La ministre des solidarités et de la santé et le ministre de l'économie et des finances,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la santé publique, notamment son article L. 1111-8 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2008-776 du 4 août 2008 modifiée de modernisation de l'économie, notamment son article 137 ;

Vu le décret n° 2008-1401 du 19 décembre 2008 modifié relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie ;

Vu le décret n° 2009-697 du 16 juin 2009 modifié relatif à la normalisation, notamment son article 17 ;

Vu le décret 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel ;

Vu l'avis n° 2017-271 du 12 octobre 2017 de la Commission nationale de l'informatique et des libertés,

Arrêtent :

Art. 1er. – Le référentiel relatif à l'accréditation des organismes de certification pour l'hébergement de données de santé à caractère personnel, mentionné à l'article R. 1111-10 du code de la santé publique, annexé au présent arrêté est approuvé.

Art. 2. – Le référentiel relatif à la certification pour l'hébergement de données de santé à caractère personnel, mentionné à l'article R. 1111-10 du code de la santé publique, annexé au présent arrêté est approuvé.

Art. 3. – Le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique est l'autorité compétente au sens du référentiel mentionné à l'article 1er du présent arrêté.

Art. 4. – Les référentiels mentionnés aux articles 1er et 2 sont disponibles sur le site internet du groupement d'intérêt public mentionné à l'article 1111-24 du code de la santé publique (www.esante.gouv.fr).

Art. 5. – La ministre des solidarités et de la santé et le ministre de l'économie et des finances sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le 11 juin 2018.

La ministre des solidarités et de la santé,
AGNÈS BUZYN

Le ministre de l'économie et des finances,
BRUNO LE MAIRE

ANNEXES

ANNEXE 1

Documents de référence
Référence n°1 : NF ISO/CEI 27001:2013 *Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences* **Référence n°2 : ISO/CEI 27018:2014** *Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII* **Référence n°3 : NF ISO/CEI 20000-1:2011** *Technologies de l'information – Gestion des services – Partie 1 Exigences du système de management des services* **Référence n°4 : Référentiel d'accréditation HDS**

Sommaire

1.Introduction

1.1. Objet du document

Le présent document constitue le référentiel de certification applicable aux hébergeurs souhaitant obtenir une certification sur le périmètre « hébergeur d'infrastructure physique » ou « hébergeur infogéreur »[1] de données de santé à caractère personnel.

Dans la suite du document, ce référentiel hébergeur de données de santé est désigné par le terme référentiel HDS.

1.2. Structure du document

Ce document est organisé en quatre parties :

1. introduction ;
2. présentation des normes internationales retenues dans le cadre de la certification pour l'hébergement de données de santé à caractère personnel ;
3. liste des acronymes utilisés dans le référentiel de certification HDS ;
4. liste des exigences du référentiel HDS portant sur les deux périmètres de certification « hébergeur d'infrastructure physique » ou « hébergeur infogéreur ».

[1] Les périmètres « hébergeur d'infrastructure physique » et « hébergeur infogéreur » sont décrits dans le document : Référentiel d'accréditation HDS – Référence n°5.

2.Références normatives

La liste des normes référencées dans ce document est présentée ci-dessous.

NF ISO/CEI 27001 Décembre 2013, *Technologies de l'information - Technique de sécurité - Systèmes de management de la sécurité de l'information - Exigences*

NF ISO/CEI 20000-1 Juin 2012, *Technologies de l'information - Gestion des services - Partie 1 : Exigences du système de management des services*

ISO/IEC 27018:2014, *Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

Pour des raisons de facilité de lecture, dans la suite du document, les références aux normes ci-dessus se feront de la manière suivante :

- NF ISO 27001 pour la norme NF ISO/CEI 27001 Décembre 2013 ;
- NF ISO 20000-1 pour la norme NF ISO/CEI 20000-1 Juin 2012 ;
- ISO 27018 pour la norme ISO/CEI 27018:2014.

3.Acronymes utilisés

DdA	Déclaration d'Applicabilité documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au SMSI d'un organisme
HDS	Hébergeur de Données de Santé
CEI	Commission électrotechnique internationale
ISO	International Organization for Standardization
OC	Organisme de Certification
SMSI	Système de Management de la Sécurité de l'Information

4. Exigences du référentiel de certification HDS

Ce chapitre énumère les exigences du référentiel HDS.

4.1. Liens entre les exigences et les normes

Les exigences du référentiel HDS définies ci-après sont d'une part, issues de normes existantes et d'autre part des exigences définies spécifiquement pour la certification HDS.

Le référentiel HDS comprend ainsi :

- les exigences de la norme NF ISO 27001 reprise dans son intégralité ;
- une partie des exigences énumérées dans la norme NF ISO 20000-1 ;
- des exigences complémentaires aux normes NF ISO 27001 et NF ISO 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.

4.2. Exigences NF ISO 27001

Les hébergeurs d'infrastructure physique et les hébergeurs infogéreurs doivent être certifiés NF ISO 27001.

En outre, les exigences spécifiques suivantes complétant la norme NF ISO 27001 s'appliquent.

Exigence complémentaire (chapitre 4.3 de la norme NF ISO 27001)

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit déterminer le domaine d'application du SMSI en tenant compte de l'objectif de protection des données de santé à caractère personnel en plus des enjeux et exigences déjà considérés.

Ce domaine d'application doit au moins couvrir l'ensemble des activités d'hébergement de données de santé à caractère personnel de l'hébergeur.

Exigence complémentaire (chapitre 6.1.3 de la norme NF ISO 27001)

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : La DdA (déclaration d'applicabilité) du SMSI doit inclure l'ensemble des exigences du référentiel de certification HDS.

Toute exclusion d'exigences, du périmètre de certification, doit être formellement justifiée et la justification doit être approuvée par l'organisme de certification.

Exigence complémentaire (Annexe A12.3 de la norme NF ISO 27001)

Application : Hébergeurs infogéreurs

Objectif : En cas d'externalisation des sauvegardes de données de santé, quel qu'en soit le support, l'hébergeur doit en garantir la sécurité.

Préconisations de mise en œuvre :

- le SMSI prend en compte les sauvegardes de données de santé, notamment leur sécurité sur les critères de confidentialité, intégrité et traçabilité lors des transferts et pendant leur conservation ;
- les mesures de sécurité des sauvegardes sont mises en œuvre.

Exigence complémentaire (Annexe A12.7 de la norme NF ISO 27001)

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit permettre à ses clients d'effectuer des audits sur les applications mises en production.

Méthode de contrôle :

- s'assurer que l'hébergeur infogéreur a défini, documenté et mis en œuvre une procédure encadrant la réalisation des audits de ses clients, en particulier les audits de sécurité (test d'intrusion, etc.) ;
- les éléments relevant de la responsabilité de l'hébergeur, en particulier des éléments mutualisés, peuvent être exclus du périmètre d'audit des clients ; dans ce cas, il convient de s'assurer que l'hébergeur est en mesure de fournir à ses clients les résultats d'un audit externe indépendant sur ces éléments.

4.3. Exigences NF ISO 20000-1

Dans le cadre de la certification HDS, seules les exigences de la norme NF ISO 20000-1 listées ci-dessous s'appliquent.

4.3.1. Planification de nouveaux services ou de services modifiés

Le chapitre 5.2 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.3.2. Conception et implémentation des nouveaux services ou des services modifiés

4.3.2.1. Présentation des activités exécutées par les fournisseurs de services, clients et autres parties

Le chapitre 5.3 (b) de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante complémentaire à la norme NF ISO 20000-1 s'applique.

Exigence complémentaire (chapitre 5.3 de la norme NF ISO 20000-1)

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit définir des critères d'acceptation pour tout nouveau service ou pour toute modification de service et réaliser des tests d'acception avant leur mise en production.

Méthode de contrôle :

- s'assurer que l'hébergeur infogéreur a mis en place une méthodologie de vérification des applications qu'il héberge ;
- vérifier que l'hébergeur infogéreur a formalisé une procédure permettant de définir les prérequis à l'hébergement et une procédure de vérification de ces prérequis (ces prérequis doivent comporter, a minima, le manuel d'installation et le manuel d'exploitation) ;
- vérifier que l'hébergeur infogéreur a formalisé un processus structuré de test et de validation permettant d'apporter la preuve objective que le futur service ne perturbera pas les performances globales du système hébergé et n'amoindrira pas son niveau de sécurité.

4.3.3. Continuité de services et gestion de la disponibilité

4.3.3.1. Exigences de continuité et de disponibilité de services

Le chapitre 6.3 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.3.3.2. Gestion de la capacité

Le chapitre 6.5 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4. Exigences relatives à la protection des données de santé à caractère personnel

Les exigences listées ci-après relatives à la protection des données de santé à caractère personnel s'appliquent. L'hébergeur ayant mis en œuvre les dispositifs et mesures spécifiés dans la norme ISO 27018 sera présumé satisfaire aux exigences dites principales. Cette présomption de conformité ne couvre pas les exigences dites complémentaires.

4.4.1. Droits des personnes

4.4.1.1. Obligation de coopérer

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit mettre à disposition les procédures et moyens pour permettre à ses clients de répondre aux demandes d'exercice des droits des personnes concernées. Les droits couverts sont ceux définis par les articles 15 à 22 du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016.

4.4.2. Finalité

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur traite les données à caractère personnel uniquement sur instruction documentée du client et ne doit pas déroger aux finalités précisées dans les instructions. Ces instructions doivent être documentées dans le cadre du contrat passé avec le client.

Exigence complémentaire

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur ne doit pas utiliser les données de santé qu'il héberge à d'autres fins que l'exécution de la prestation d'hébergement. Est notamment interdite, toute utilisation de ces données à des fins marketings, publicitaires, commerciales, ou statistiques.

4.4.3. Communication des données

4.4.3.1. Données temporaires

Exigence principale

Application : Hébergeurs infogéreurs.

Objectif : L'hébergeur doit définir une période de rétention des données temporaires et respecter ce délai. L'hébergeur doit documenter et mettre en place les moyens permettant de s'assurer que les données temporaires sont effacées à expiration de ce délai.

4.4.3.2. Notification en cas de communication de données à caractère personnel

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les saisies judiciaires incluant des données à caractère personnel doivent être encadrées au niveau contractuel. Une procédure doit définir les modalités de notification du client d'une telle transmission, sauf à ce que cette notification soit interdite.

4.4.3.3. Traçabilité en cas de communication

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit assurer la journalisation de la transmission des données à caractère personnel à des tiers avec a minima les informations suivantes : la liste des données transmises, le ou les destinataires et les dates de communication.

4.4.3.1. Intégrité et acquittement des échanges

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les données à caractère personnel transitant par un réseau de communication doivent faire l'objet de contrôles permettant de s'assurer que ces données sont bien reçues par le système cible.

4.4.4. Transparence

4.4.4.1. Obligation d'information en cas de sous-traitance

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les clauses contractuelles passées entre l'hébergeur et son client doivent préciser le recours éventuel à un sous-traitant dans le cadre du traitement des données à caractère personnel. Ainsi, l'hébergeur ne doit pas faire appel à un sous-traitant sans l'information préalable du client.

4.4.5. Responsabilité

4.4.5.1. Notification en cas d'atteinte à la sécurité des données

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur notifie son client de toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

4.4.5.2. Période de conservation des politiques de sécurité

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les durées de rétention des différentes versions du corpus documentaire sécurité doivent être définies et formalisées.

4.4.5.3. Gestion des informations personnelles

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'hébergeur doit avoir défini et formalisé une politique encadrant la mise à disposition et la restitution des données à caractère personnel à ses clients, ainsi que leur destruction. Cette politique doit être communiquée au client sur demande.

Exigence complémentaire

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : Une procédure de réversibilité définissant les modalités de restitution des données en fin de contrat ou retrait de la certification doit être formalisée et appliquée.

4.4.6. Sécurité des données

4.4.6.1. Les accords de confidentialité ou de non-divulgation

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : Les contrats de travail des salariés de l'hébergeur doivent inclure une clause de confidentialité. En cas de recours à la sous-traitance, cette exigence s'applique également aux prestataires.

4.4.6.2. Restriction sur l'usage de copies papier

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'hébergeur doit restreindre le recours à des copies papier.

4.4.6.3. Contrôle et traçabilité lors de la restauration de données

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'hébergeur doit disposer d'une procédure encadrant la restauration des données. Les opérations de restauration effectuées doivent être journalisées.

4.4.6.4. Protection des données présentes sur un support de stockage en dehors du lieu d'hébergement

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Si des supports de stockage portables contenant des données à caractère personnel sont sortis des locaux de l'hébergeur, une autorisation préalable devra être obtenue. Ces données ne doivent pas être accessibles à du personnel non autorisé, par exemple en les protégeant par des solutions de chiffrement à l'état de l'art.

4.4.6.5. Utilisation de support de stockage portable

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'utilisation de supports de stockage portables incompatibles avec des solutions de chiffrement doit être proscrite.

4.4.6.6. Chiffrement des données personnelles transmises sur des réseaux publics

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les données à caractère personnel doivent être chiffrées avant d'être transmises sur des réseaux publics.

4.4.6.7. Destruction des copies papier

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : La destruction des copies papier doit être effectuée avec des moyens appropriés.

4.4.6.8. Utilisation d'identifiants uniques

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement doit être réalisé à l'aide de comptes nominatifs.

Exigence complémentaire

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Des moyens de traçabilité doivent être mis en œuvre afin de contrôler les actions et les usages des identifiants génériques.

Méthode de contrôle :

L'organisme de certification doit :

- s'assurer que la politique de gestion des comptes génériques limite leur usage à des cas particuliers et identifiés, par exemple en raison de contraintes intrinsèques de certains équipements ou logiciels ;
- s'assurer que les traces nominatives et horodatées d'utilisation des comptes génériques sont incluses dans la politique de gestion des traces.

4.4.6.9. Gestion des habilitations

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Un processus de gestion des habilitations doit être défini et appliqué avec notamment la tenue d'un registre actualisé des utilisateurs ou profils utilisateurs ayant accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement.

4.4.6.10. Gestion des traces

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit mettre en œuvre les moyens d'assurer la traçabilité des actions des utilisateurs, des défaillances et des événements liés à la sécurité de l'information. Les journaux contenant les traces doivent être conservés et revus régulièrement. L'hébergeur doit assurer l'intégrité des journaux et les protéger des accès illicites.

En complément, les activités des administrateurs système et des opérateurs techniques doivent être tracées ; les journaux associés doivent être protégés et revus régulièrement.

Afin de garantir la fiabilité des journaux, l'hébergeur doit s'assurer de la synchronisation de l'ensemble des horloges des systèmes (référence temporelle unique).

Exigence complémentaire

Application : Hébergeurs infogéreurs

Objectif : Des moyens techniques et organisationnels doivent être mis en œuvre afin de communiquer au client les traces des administrateurs.

Méthode de contrôle :

- s'assurer que l'hébergeur a formalisé et mis en œuvre les moyens organisationnels et techniques permettant de traiter les demandes de ses clients relatives aux traces d'accès des administrateurs de l'hébergeur aux systèmes d'information de santé hébergés.

4.4.6.11. Gestion des identifiants

Exigence principale

Application : Hébergeurs infogéreurs.

Objectif : Les comptes désactivés ou expirés ne doivent pas être réattribués à de nouvelles personnes.

4.4.6.12. Clauses contractuelles

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Les contrats passés entre l'hébergeur et ses clients doivent spécifier les mesures techniques et organisationnelles prévues pour répondre aux objectifs de sécurité et de protection des données à caractère personnel, ainsi que les finalités de traitement. Des changements dans ces mesures ne doivent pas aboutir à une réduction du niveau de sécurité, sauf accord préalable du client.

4.4.6.13. Sous-traitance du traitement des données personnelles

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : En cas de recours par l'hébergeur à la sous-traitance, le contrat afférent doit spécifier les mesures techniques et organisationnelles prévues pour répondre aux objectifs de sécurité et de protection des données à caractère personnel. Des changements dans ces mesures ne doivent pas aboutir à une réduction du niveau de sécurité, sauf accord préalable de l'hébergeur. L'hébergeur doit s'assurer que ce niveau de sécurité respecte les engagements pris avec ses clients.

4.4.6.14. Réutilisation des espaces de stockage

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit s'assurer qu'en cas de réaffectation d'espaces de stockage, ceux-ci ont bien été préalablement purgés et qu'aucune ancienne donnée ne peut être accédée.

4.4.7. Localisation des données

4.4.7.1. Lieux d'hébergement

Exigence principale

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit spécifier la liste de l'ensemble des pays au sein desquels les données du client sont ou peuvent être hébergées.

Exigence complémentaire

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit informer son client des lieux d'hébergement et lui permettre de choisir le(s) pays d'hébergement dans le(s)quel(s) les données de santé seront hébergées et mettre en œuvre les mesures permettant de respecter ce choix.

4.5. Exigences complémentaires

4.5.1. Rôles et responsabilités

Application : Hébergeurs d'infrastructure physique, hébergeurs infogéreurs.

Objectif : La répartition des responsabilités en termes de sécurité de l'information entre l'hébergeur et son client doit être définie et formalisée.

4.5.2. Conformité aux référentiels opposables de la PGSSI-S

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit informer ses clients qu'ils sont tenus de respecter la PGSSI-S (politique générale de sécurité des systèmes d'information de santé) et doit mettre en place un moyen de recueillir l'engagement de ce respect.

Méthode de contrôle :

- l'hébergeur doit informer ses clients qu'ils sont tenus de mettre en œuvre un système d'information de santé respectant la PGSSI-S ;
- l'hébergeur doit définir et mettre en place un moyen de recueillir l'engagement de ses clients de respecter les référentiels opposables de la PGSSI-S. Cet engagement pourrait être encadré dans le contrat d'hébergement.

4.5.3. Rapports d'audit

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit communiquer les rapports d'audit de certification aux clients qui en font la demande. Il doit également fournir ces rapports à l'organisme de certification, en cas de transfert ou de demande d'équivalence.

4.5.4. Liste des contacts clients

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit maintenir une liste des points de contact pour chacun des clients.

Ce point de contact doit être en mesure de désigner à l'hébergeur un professionnel de santé lorsque cela est nécessaire (exemples : accès aux données de santé, gestion des relations avec le patient, etc.)

L'hébergeur doit être en capacité de transmettre sans délai cette liste à l'autorité compétente sur demande, notamment en cas de suspension ou de retrait de la certification.

Méthode de contrôle :

- vérifier que la liste de contacts des clients de l'hébergeur contient, a minima, les informations suivantes :
  - la raison sociale du client ;
  - les nom et prénom du contact ;
  - l'adresse mail du contact ;
  - le numéro de téléphone du contact ;
- vérifier que cette liste est mise à jour régulièrement.

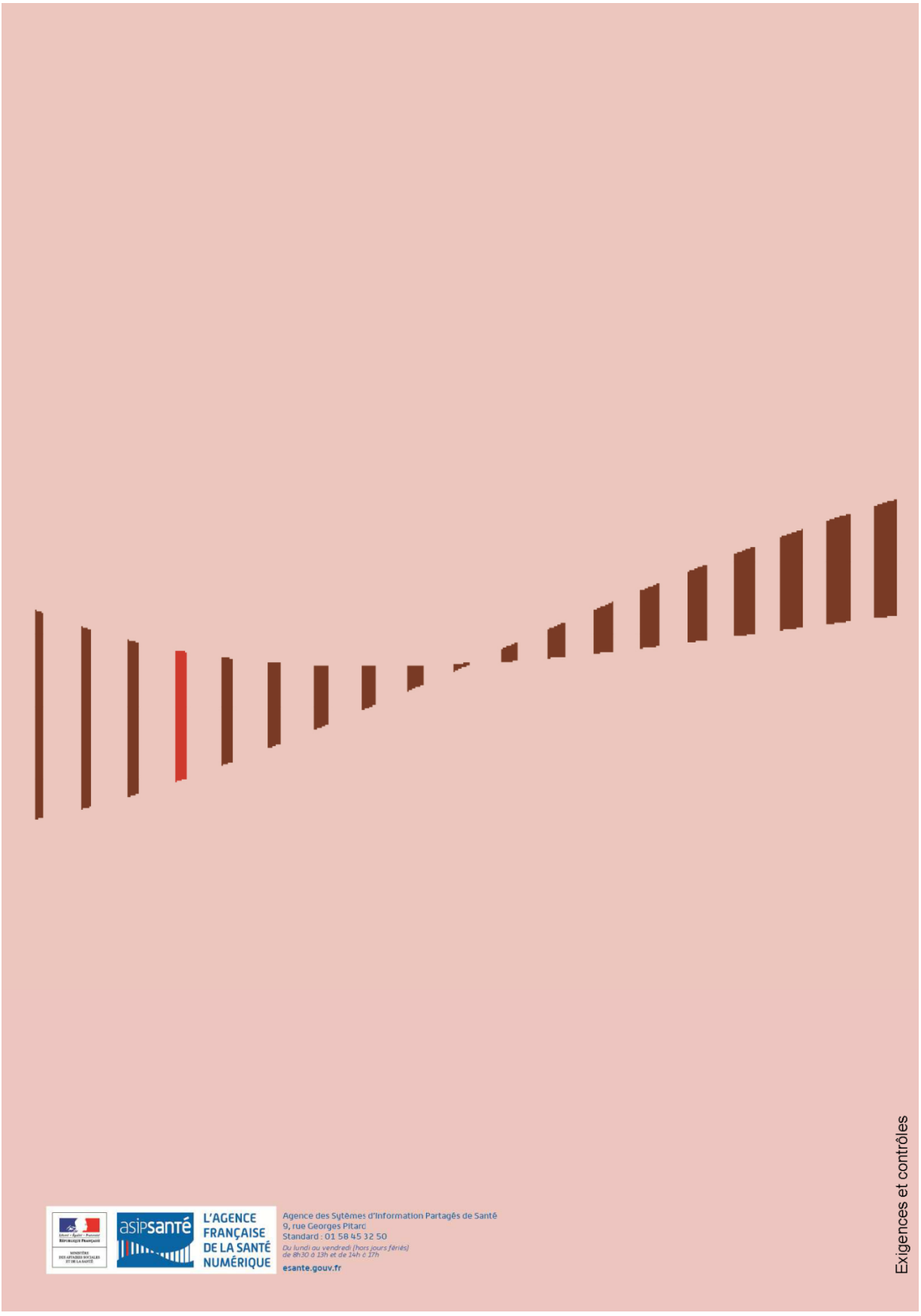
4.5.5. Régionalisation

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

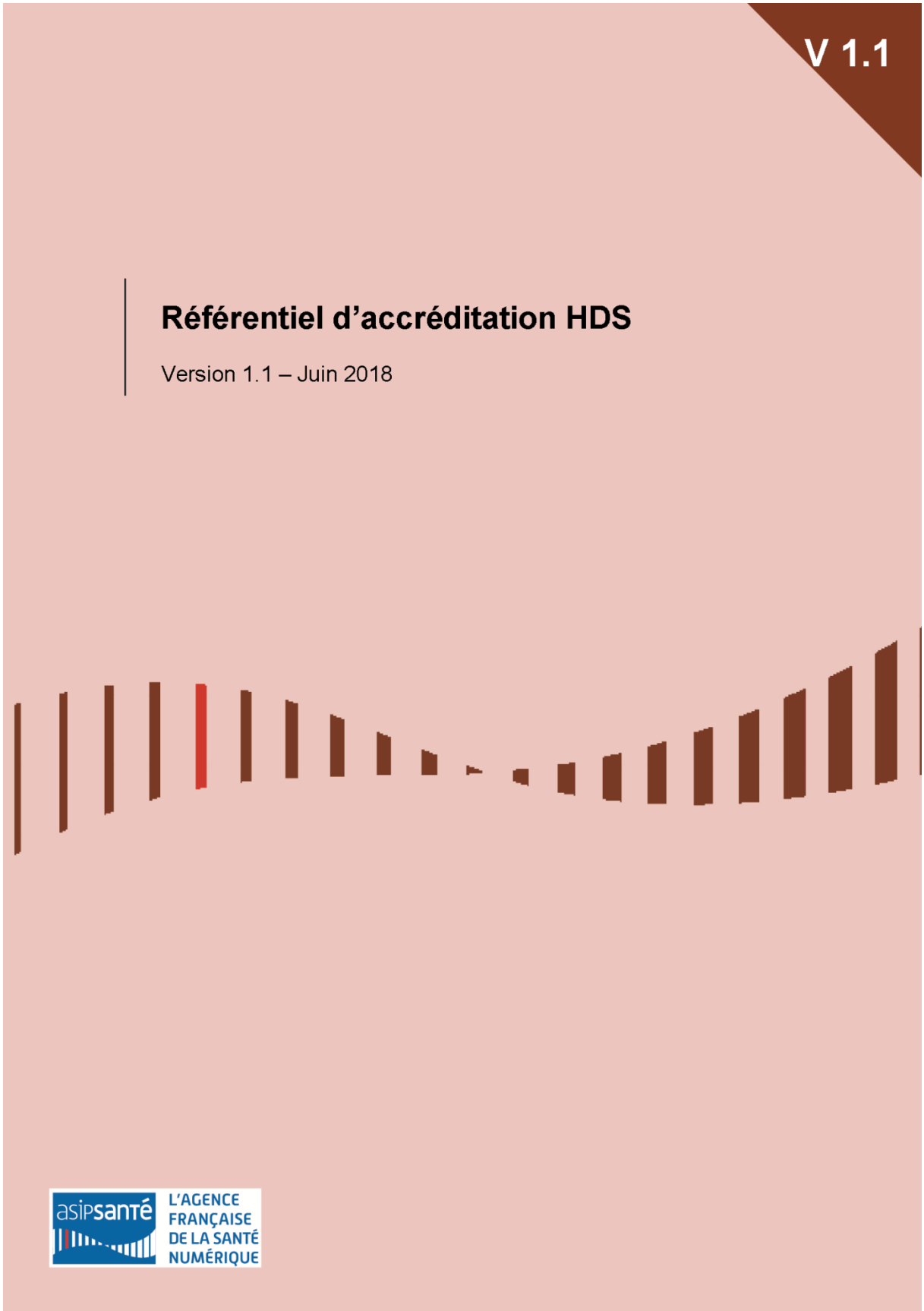
Objectif : Régionalisation des relations avec le client.

Méthode de contrôle :

- s'assurer que les interfaces proposées aux clients sont disponibles au moins en langue française.
- l'hébergeur doit assurer un support de premier niveau au moins en langue française.
- vérifier que la DdA est disponible au moins en langue française.


asipsanté
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
Exigences et contrôles

ANNEXE 2


V 1.1
Référentiel d'accréditation HDS
Version 1.1 – Juin 2018
asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Documents de référence

Référence n°1 : NF ISO/CEI 17021-1:2015
Évaluation de la conformité -- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management

Référence n°2 : NF ISO/CEI 27001:2013
Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences

Référence n°3 : NF ISO/CEI 20000-1:2011
Technologies de l'information – Gestion des services – Partie 1 Exigences du système de management des services

Référence n°4 : Exigences et contrôles du référentiel HDS

Référence n°5 : IAF MD1:2018
Document d'exigences IAF pour la certification multi-sites par échantillonnage

Référence n°6 : IAF MD2:2017
Document d'exigences IAF pour le transfert d'une certification sous accréditation de systèmes de management

Référence n°7 : IAF MD4:2008
Document d'exigences IAF pour l'utilisation de techniques d'audit assistées par ordinateur (« TAAO ») pour la certification sous accréditation de systèmes de management

Référence n°8 : IAF MD5:2015
Détermination du temps d'audit des systèmes de management de la qualité et des systèmes de management environnemental

Référence n°9 : IAF MD11:2013
Document d'exigences IAF pour l'application de la norme ISO/CEI 17021 pour les audits de Systèmes de Management Intégrés (SMI)

Sommaire

1.Introduction

1.1. Objet du document

Ce document s'adresse aux organismes de certification souhaitant être accrédités pour la certification « hébergeur d'infrastructure physique » ou « hébergeur infogéreur » et aux hébergeurs souhaitant obtenir une certification. Il décrit le processus d'accréditation des organismes de certification et le processus de certification des hébergeurs.

1.2. Structure du document

Ce document est organisé en sept parties et quatre annexes :

1. introduction du document ;
2. description du champ d'application du référentiel d'accréditation ;
3. description des normes applicables au sein du référentiel d'accréditation ;
4. liste des acronymes utilisés dans le référentiel d'accréditation ;
5. description des conditions, critères et modalités d'accréditation des organismes de certification ;
6. définition des responsabilités des organismes d'accréditation ;
7. description des conditions, critères et modalités de certification des hébergeurs ;

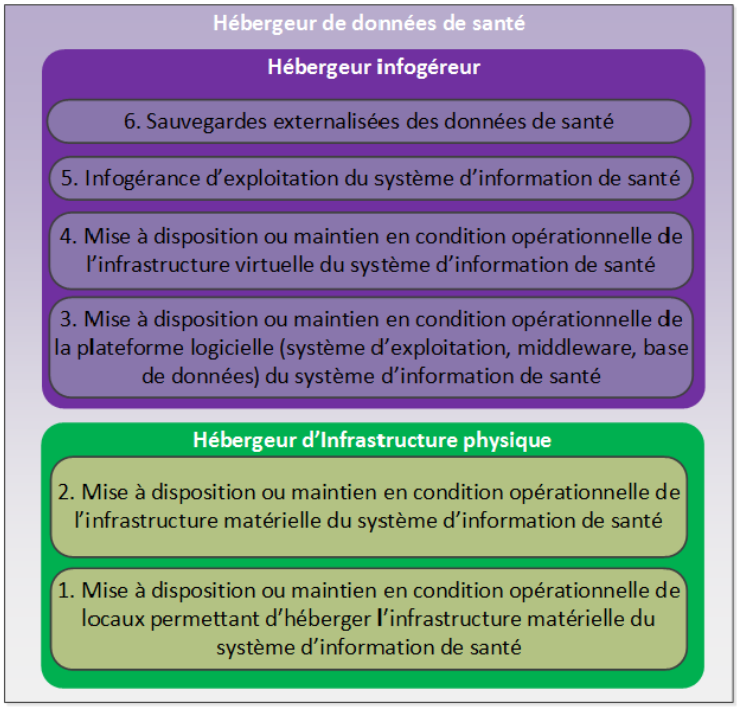
Annexes

1. annexe A présentant les éléments nécessaires permettant de déterminer la durée d'audit pour la certification HDS ;
2. annexe B présentant les modèles de documents à utiliser par les organismes de certification pour envoyer des informations à l'autorité compétente ;
3. annexe C présentant le modèle de notification de suspension de certification ;
4. annexe D présentant le modèle de notification de retrait de certification.

2. Domaine d'application

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 suivantes :

1. la mise à disposition et le 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 ;
2. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. la mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
4. la mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
5. l'administration et l'exploitation du système d'information contenant les données de santé ;
6. la sauvegarde de données de santé.



Un hébergeur souhaitant obtenir une certification pour l'hébergement de données de santé doit identifier les activités concernées par sa demande de certification.

Lorsque le périmètre d'activités comprend uniquement les activités numérotées 1 et/ou 2, l'hébergeur est évalué pour la conformité aux exigences s'appliquant aux hébergeurs d'infrastructure physique. La certification obtenue est dénommée certification « hébergeur d'infrastructure physique ».

Lorsque le périmètre d'activités comprend uniquement les activités numérotées de 3 à 6, l'hébergeur est évalué pour la conformité aux exigences s'appliquant aux hébergeurs infogéreurs. La certification obtenue est dénommée certification « hébergeur infogéreur ».

Lorsque le périmètre pour lequel l'hébergeur souhaite obtenir la certification comprend au moins une activité appartenant aux deux périmètres de certification, l'hébergeur est évalué pour la conformité à toutes les exigences et obtient les deux périmètres de certification.

Dans la suite du document, le terme « certification HDS » peut désigner indifféremment l'un ou l'autre de ces périmètres de certification.

3.Références normatives

Les documents, listés ci-dessous sont référencés de manière normative dans le présent référentiel et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NF ISO/CEI 27001:2013, *Technologies de l'information - Technique de sécurité - Systèmes de management de la sécurité de l'information - Exigences*

NF ISO/CEI 20000-1:2011, *Technologies de l'information - Gestion des services - Partie 1 : Exigences du système de management des services*

NF ISO/CEI 17021-1:2015, *Évaluation de la conformité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences*

Dans la suite du document, les références à ces normes se feront de la manière suivante :

- NF ISO 27001 pour la norme NF ISO/IEC 27001:2013 ;
- NF ISO 20000-1 pour la norme NF ISO/IEC 20000-1:2011 ;
- NF ISO 17021-1 pour la norme NF ISO/IEC 17021-1:2015.

4.Acronymes utilisés

COFRAC	Comité Français d'Accréditation
DdA	Déclaration d'Applicabilité documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au Système de Management de la Sécurité de l'Information d'un organisme
HDS	Hébergeur de Données de Santé
IAF	International Accreditation Forum
CEI	Commission Electrotechnique Internationale
ISO	International Organization for Standardization
OC	Organisme de Certification

5.Conditions, critères et modalités d'accréditation

Les conditions, critères et modalités d'accréditation s'appuient sur les standards de la norme NF ISO 17021-1. L'accréditation atteste de la compétence, de l'impartialité et de la fiabilité d'un organisme à vérifier la conformité à des exigences établies et formalisées. L'accréditation constitue un contrôle dit de deuxième niveau qui vise à contrôler la façon dont opère le contrôleur.

5.1. Conditions et critères d'accréditation

Les organismes de certification habilités à délivrer des certificats de conformité HDS doivent être accrédités par une instance nationale d'accréditation telle que définie dans le règlement CE 765/2008 (le COFRAC en France ou son équivalent dans les autres pays signataires des accords multilatéraux de reconnaissance internationaux) conformément au présent référentiel d'accréditation qui sera revu régulièrement afin d'intégrer notamment les évolutions technologiques au sein des systèmes d'information de santé, ainsi que les mutations des métiers de l'hébergement.

L'application et le respect des exigences du référentiel d'accréditation permettent de garantir que les organismes accrédités sont compétents pour délivrer les certifications HDS.

L'accréditation porte sur l'évaluation des organismes souhaitant être certifiés hébergeurs de données de santé à caractère personnel.

Pour qu'un organisme puisse être accrédité pour délivrer des certifications HDS, il doit remplir les conditions décrites dans la norme NF ISO 17021-1 et appliquer les règles en vigueur pour l'audit et la certification des systèmes de management de la sécurité des systèmes d'information. En outre, le présent référentiel d'accréditation définit les exigences spécifiques qui s'appliquent à la certification HDS.

5.2. Exigences d'accréditation

5.2.1. Exigences générales

5.2.1.1. Domaine contractuel et juridique

Les exigences du §5.1 de la norme NF ISO 17021-1 s'appliquent.

5.2.1.2. Gestion de l'impartialité

Les exigences du §5.2 de la norme NF ISO 17021-1 s'appliquent.

5.2.1.3. Responsabilité et financement

Les exigences du §5.3 de la norme NF ISO 17021-1 s'appliquent.

5.2.2. Exigences structurelles

5.2.2.1. Compétence du personnel

Les exigences du §7.1 de la norme NF ISO 17021-1 s'appliquent.

Lors de la sélection de l'équipe d'audit, l'organisme de certification veille à ce que les compétences apportées à chaque mission soient appropriées. L'équipe doit avoir une connaissance suffisante des aspects de sécurité de l'information, d'hébergement de données sensibles et des services proposés par les hébergeurs de données de santé.

En particulier, les auditeurs de l'organisme de certification qui participent aux activités de certification HDS doivent être en mesure de démontrer qu'ils possèdent des compétences dans les domaines de la sécurité des systèmes d'information et notamment des systèmes d'information de santé.

La direction de l'organisme de certification doit définir les processus et disposer des ressources nécessaires pour lui permettre de déterminer si oui ou non les auditeurs sont compétents pour les tâches qu'ils doivent accomplir dans le cadre de la certification HDS. L'organisme de certification doit être en mesure de communiquer à ses clients les compétences de son personnel impliqué dans les activités de certification.

5.2.2.2. Personnel intervenant dans les activités de certification

Les exigences du §7.2 de la norme NF ISO 17021-1 s'appliquent.

L'équipe d'auditeurs peut être renforcée par des experts techniques. Ces experts techniques ne se substituent pas aux auditeurs, mais accompagnent ces derniers sur les questions d'adéquation entre la sécurité et les dispositifs utilisés dans le contexte de l'hébergement de données de santé.

Il est recommandé que les experts aient des compétences spécifiques dans le domaine de la santé acquises à l'occasion d'une formation ou d'un projet.

L'organisme de certification doit avoir une procédure permettant :

a) de sélectionner des auditeurs et des experts techniques sur la base de leurs compétences, leurs formations, leurs qualifications et leur expérience ;
b) d'évaluer la conduite des auditeurs et des experts techniques lors des audits de certification et de surveillance.

5.2.2.3. Intervention d'auditeurs et d'experts techniques externes individuels

Les exigences du §7.3 de la norme NF ISO 17021-1 s'appliquent.

5.2.2.4. Enregistrements relatifs au personnel

Les exigences du §7.4 de la norme NF ISO 17021-1 s'appliquent.

5.2.2.5. Externalisation

Les exigences du §7.5 de la norme NF ISO 17021-1 s'appliquent.

5.2.3. Exigences relatives aux informations

5.2.3.1. Informations accessibles au public

Les exigences du §8.1 de la norme NF ISO 17021-1 s'appliquent.

5.2.3.2. Documents de certification

Les exigences du §8.2 de la norme NF ISO 17021-1 s'appliquent.

L'organisme de certification fournit à chacun de ses clients certifiés hébergeurs de données de santé à caractère personnel les documents attestant de leur certification.

Ces documents doivent :

- préciser le périmètre du service certifié au regard des activités définies dans le chapitre 2 « Domaine d'application » ;
- spécifier les normes ISO pour lesquelles l'organisme est déjà certifié et dont il respecte les exigences en vigueur (NF ISO 27001 et NF ISO 20000-1).
- préciser la localisation de tous les sites entrant dans le périmètre de certification.

5.2.3.3. Référence à la certification et utilisation des marques

Les exigences du §8.3 de la norme NF ISO 17021-1 s'appliquent.

5.2.3.4. Confidentialité

Les exigences du §8.4 de la norme NF ISO 17021-1 s'appliquent.

Avant toute intervention de la part de l'équipe d'audit, l'organisme de certification doit s'assurer avec le candidat que les informations qui seront communiquées durant l'audit ne contiennent aucune donnée de santé à caractère personnel, ni aucune donnée confidentielle ou sensible. Le cas échéant, l'organisme de certification et le candidat doivent définir les modalités d'accès au système devant être audité (engagement de confidentialité, etc.).

Dans le cas d'une incapacité à auditer le système d'information sans accéder à des données de santé à caractère personnel ou d'autres données confidentielles ou sensibles, l'organisme de certification doit en informer le candidat, un accord de confidentialité doit être établi et un professionnel de santé intervenant sous la responsabilité du client doit être informé.

Le chapitre 8.4.2 de la norme NF ISO 17021-1 est complété ainsi : les données de santé à caractère personnel et toutes autres données confidentielles ou sensibles auxquelles l'organisme de certification aurait accès dans le cadre de l'audit ne peuvent être divulguées ou réutilisées par l'organisme de certification, ni par le candidat à la certification.

Les accès éventuels à des données de santé par l'organisme de certification doivent être tracés. Ces traces doivent être horodatées et comporter l'identification nominative de l'auditeur.

5.2.3.5. Echanges d'informations avec l'autorité compétente

a. Rapport de suspension HDS

L'organisme de certification doit communiquer en français ou en anglais à l'autorité compétente toute décision de suspension de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été suspendue doivent être communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été suspendue ;
- numéro d'identifiant du certificat suspendu ;
- date de suspension du certificat ;
- raisons de la suspension de la certification HDS.

L'envoi des informations doit être réalisé par voie électronique en complétant le modèle proposé en Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

b. Rapport de retrait HDS

L'organisme de certification doit communiquer en français ou en anglais à l'autorité compétente toute décision de retrait de certification d'un hébergeur de données de santé.

Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été retirée doivent être communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été retirée ;
- numéro d'identifiant du certificat retiré ;
- date de retrait du certificat ;
- raisons du retrait de la certification HDS.

L'envoi des informations doit être réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

c. Répertoire clients HDS

L'organisme de certification doit fournir mensuellement un rapport des certifications valides, suspendues et retirées, à l'autorité compétente. Ce rapport, en français ou en anglais, doit contenir les données suivantes pour chaque hébergeur de données de santé :

- désignation ou raison sociale de l'hébergeur de données de santé ;
- numéro d'identifiant du certificat ;
- type de certificat ;
- périmètre de la certification ;
- adresse du site certifié et dans le cas d'une certification multi-sites, indiquer l'adresse du siège social, ainsi que celles de tous les sites rattachés ;
- état de la certification (valide, suspendue ou retirée) ;
- date de la certification.

L'envoi du répertoire doit être réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

d. Rapport annuel HDS

Les exigences du § 8.5 de la norme NF ISO 17021-1 s'appliquent.

Chaque année, l'organisme de certification doit fournir à l'autorité compétente un rapport annuel en français ou en anglais comprenant :

- une synthèse anonymisée des certifications HDS, des audits réalisés et des non-conformités relevées.
- une synthèse des difficultés rencontrées lors de la certification des hébergeurs et des éventuelles propositions de modifications à apporter aux référentiels de certification et d'accréditation ;
- des indicateurs sur la procédure de certification HDS, tels que :
  - nombre d'hébergeurs de données de santé en cours de certification ;
  - nombre d'hébergeurs de données de santé ayant échoué à la certification ;
  - nombre de renouvellements de certification ;
  - durée moyenne des audits.

L'envoi du rapport annuel doit être réalisé par voie électronique entre le 1er et le 31 janvier de l'année suivante, en complétant le modèle proposé en Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

5.2.4. Exigences du processus de certification

5.2.4.1. Activités préalables à la certification

a. Demande de certification

Les exigences du § 9.1.1 de la norme NF ISO 17021-1 s'appliquent.

Dans le cas d'un transfert de certificat, le guide IAF MD 2:2017[1] s'applique. En complément, l'organisme de certification récepteur devra informer l'autorité compétente de tout transfert de certificat et indiquer le nom de l'organisme de certification émetteur.

b. Revue de la demande

Les exigences du § 9.1.2 de la norme NF ISO 17021-1 s'appliquent.

c. Programme d'audit

Les exigences du § 9.1.3 de la norme NF ISO 17021-1 s'appliquent.

Le chapitre 9.1.3.5 est complété par l'exigence suivante : la description du périmètre de certification doit préciser la liste des activités énumérées au chapitre 2 pour lesquelles le candidat demande une certification afin de déterminer le type de certification HDS.

Les exigences applicables pour chacun des types de certification (certification « hébergeur d'infrastructure physique » et certification « hébergeur infogéreur ») sont précisées dans le document décrivant les exigences et contrôles du référentiel HDS.

d. Détermination du temps d'audit

Les exigences du § 9.1.4 de la norme NF ISO 17021-1 s'appliquent. En complément, les exigences des guides IAF MD 4:2008[2] et MD 5:2015[3] s'appliquent.

La détermination de la durée d'audit doit être réalisée en appliquant la méthode et les tableaux, de l'« Annexe A : Tableau de durée d'audit pour la certification HDS » du présent document.

Si après calculs le résultat obtenu n'est pas un nombre entier, le nombre de jours doit être arrondi à la demi-journée la plus proche (par ex. : 5,3 jours d'audit deviennent 5,5 jours d'audit, et 5,2 jours d'audit deviennent 5 jours d'audit).

e. Echantillonnage multiple

Les exigences du § 9.1.5 de la norme NF ISO 17021-1 s'appliquent. En complément, le guide IAF MD 1:2018[4] s'applique.

f. Normes de systèmes de management multiples

Les exigences du § 9.1.6 de la norme NF ISO 17021-1 s'appliquent, ainsi que le guide IAF MD 11:2013[5].

5.2.4.2. Planification des audits

Les exigences du § 9.2 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.3. Certification initiale

Les exigences du § 9.3 de la norme NF ISO 17021-1 s'appliquent.

[1] https://www.cofrac.fr/documentation/IAF-MD2
[2] https://www.cofrac.fr/documentation/IAF-MD4
[3] https://www.cofrac.fr/documentation/IAF-MD5
[4] https://www.cofrac.fr/documentation/IAF-MD1
[5] https://www.cofrac.fr/documentation/IAF-MD11

5.2.4.4. Réalisation des audits

Les exigences du § 9.4 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.5. Décision de certification

Les exigences du § 9.5 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.6. Maintien de la certification

Les exigences du § 9.6 de la norme NF ISO 17021-1 s'appliquent.

La certification est délivrée pour une durée de 3 ans. Les hébergeurs certifiés doivent déposer auprès de l'organisme de certification une demande de recertification au plus tard 3 mois avant la date de fin de validité de la certification.

5.2.4.7. Appels

Les exigences du § 9.7 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.8. Plaintes

Les exigences du § 9.8 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.9. Enregistrements relatifs au client

Les exigences du § 9.9 de la norme NF ISO 17021-1 s'appliquent.

5.2.4.10. Exigences du système de management pour les organismes de certification

a. Options

Les exigences du § 10.1 de la norme NF ISO 17021-1 s'appliquent.

b. Exigences du système de management conformément à la norme ISO 9001

Les exigences du § 10.2 de la norme NF ISO 17021-1 s'appliquent.

c. Exigences générales du système de management

Les exigences du § 10.3 de la norme NF ISO 17021-1 s'appliquent.

5.2.5. Modalités d'évaluation

L'annexe B de la norme NF ISO 17021-1 s'applique.

6.Responsabilités des organismes d'accréditation

Les missions des organismes d'accréditation (le COFRAC, en France, et ses homologues européens), consistent à s'assurer que les organismes qu'ils accréditent sont compétents et impartiaux et qu'ils le demeurent dans le temps, quel que soit le contexte.

Pour attester de cette compétence, l'organisme d'accréditation réalise des évaluations régulières du fonctionnement de ces organismes accrédités. Les évaluations sont constituées d'une revue documentaire ainsi que d'une intervention des évaluateurs en tant que témoins d'un audit pour vérifier à la fois la qualité des procédures et la façon dont elles sont appliquées.

6.1. Processus d'accréditation

Le processus d'accréditation est conforme à la norme NF ISO 17021-1.

Si l'organisme de certification est déjà accrédité pour la norme NF ISO 17021-1, une extension majeure de la portée d'accréditation à un nouveau domaine doit être réalisée. Cela conduit à une évaluation au siège de l'organisme et au moins à une observation d'activité.

Si l'organisme de certification n'est pas déjà accrédité pour la norme NF ISO 17021-1, le processus d'accréditation initial doit être appliqué.

Après recevabilité favorable de la demande d'accréditation par l'instance nationale d'accréditation pour la certification HDS (recevabilité opérationnelle), les organismes certificateurs en cours de demande d'accréditation sont autorisés à délivrer des certificats pendant neuf (9) mois.

L'accréditation doit être obtenue dans un délai maximum de neuf (9) mois, à compter de la date de notification de la décision positive de recevabilité opérationnelle.

Si l'accréditation n'est pas obtenue dans ce délai, l'organisme de certification en informe ses clients pour qu'ils prennent contact avec un autre organisme de certification pour obtenir un nouveau certificat.

Les certificats émis pendant la période des neuf (9) mois devront être réémis sous accréditation s'ils ont été initialement délivrés dans les mêmes conditions que celles ayant permis de prononcer l'accréditation.

La portée d'accréditation est exprimée comme suit :

Objet de la certification	Référence de certification	Référentiel d'accréditation
Systèmes de management de la sécurité des systèmes d'information des hébergeurs de données de santé	Référentiel de Certification HDS Exigences et contrôles (version en vigueur)	Référentiel d'accréditation HDS (version en vigueur)

6.2. Processus de suspension de l'accréditation

6.2.1. Décision de suspension

Dans le cas d'une suspension de l'accréditation à l'initiative de l'organisme d'accréditation, ce dernier en informe sans délai l'organisme de certification et l'autorité compétente.

L'envoi de la notification de suspension doit être réalisé par voie électronique en complétant le modèle de l'Annexe C : Notification de suspension de certification.

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 lever la suspension de l'accréditation de l'organisme de certification.

Si l'organisme de certification ne transmet 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.

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

6.2.2. Levée de suspension

Dans le cas d'une suspension à l'initiative de l'organisme d'accréditation, les conditions de levée de la suspension sont spécifiées dans la décision de suspension adressée à l'organisme de certification.

La décision de levée de suspension ne peut être émise qu'à la suite d'une évaluation de l'organisme de certification sur site ou à l'examen par l'organisme d'accréditation d'un rapport d'audit interne transmis par l'organisme de certification. Si le rapport ne fournit pas d'éléments suffisants pour démontrer la conformité aux exigences d'accréditation, l'organisme de certification est informé par courrier que sa suspension ne pourra être levée qu'au vu des résultats d'une évaluation sur site. La décision de levée de suspension est notifiée par l'organisme d'accréditation. 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 par rapport à l'accréditation initiale.

En cas de refus de la levée de la suspension, l'organisme de certification peut faire appel de la décision auprès de l'organisme d'accréditation.

6.3. Processus de retrait de l'accréditation

Dans le cas d'un retrait de l'accréditation, l'organisme d'accréditation informe sans délai l'organisme de certification et l'autorité compétente, de toute mesure de retrait d'accréditation.

L'envoi de la notification de retrait à l'autorité compétente doit être réalisé par voie électronique en complétant le modèle de l'Annexe D : Notification de retrait de certification.

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 de certification par lettre recommandée avec accusé de réception, précisant les motivations de la décision.

L'organisme n'est plus autorisé à délivrer de certificats ni à maintenir les certificats existants.

L'organisme de certification 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 l'autorité compétente et ses clients pour que ces derniers puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

L'organisme d'accréditation a la possibilité d'intervenir sur le site de l'organisme de certification afin de s'assurer que les activités liées à la certification d'hébergeurs de données de santé ont été suspendues et que l'autorité compétente et les clients ont été informés.

6.4. Transfert de certification à un nouvel organisme de certification à la suite d'un retrait

Le nouvel organisme de certification qui reçoit une demande de transfert doit appliquer les dispositions décrites dans le § 7 du présent document. S'il est dans l'impossibilité de se procurer le dossier du client auprès de l'organisme précédent, la demande du client sera traitée comme une certification initiale. Dans tous les cas, il revient à l'organisme de certification « récepteur » d'évaluer les éléments fournis et d'établir si le cycle de certification peut être repris à la même étape de certification que celle dans laquelle il se trouvait avec l'organisme de certification initial.

6.5. Cessation d'activité d'un organisme de certification

L'organisme d'accréditation informe sans délai l'autorité compétente, de toute annonce de cessation d'activité d'un organisme de certification.

L'organisme de certification est également tenu d'informer l'autorité compétente, ainsi que les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

7. Conditions, critères et modalités de certification

7.1. Conditions et critères de certification

Un candidat souhaitant obtenir une certification HDS devra répondre aux exigences du référentiel de certification HDS et faire une demande de certification auprès d'un organisme de certification accrédité conformément au référentiel d'accréditation HDS.

Pour obtenir une certification HDS, un candidat doit :

- être certifié ISO 27001 sur un périmètre couvrant au moins celui pour lequel il demande une certification HDS (le candidat peut obtenir sa certification ISO 27001 dans le cadre de la certification HDS et inversement la certification HDS peut être obtenue à l'occasion d'une certification ISO 27001) ;
- prendre en compte dans son système de management de la sécurité de l'information les exigences du référentiel de certification HDS applicables au type de certificat demandé (exigences issues des normes ISO 20000-1, et des exigences relatives à la protection des données à caractère personnel et spécifiques santé).

Un hébergeur qui a déjà obtenu une certification ISO 27001 ou une certification ISO 20000-1 peut faire prévaloir ces certifications s'il remplit les conditions citées dans le chapitre 7.2.

Un candidat disposant déjà de ces certifications est évalué sur le périmètre des exigences du référentiel de certification non couvertes par ces certifications. Les certifications déjà obtenues font l'objet d'une vérification selon les modalités définies au chapitre 7.2.

7.2. Equivalence

Si le candidat souhaite faire prévaloir la ou les certification(s) selon les normes NF ISO 27001 et NF ISO 20000-1 qu'il a déjà obtenues, ces certifications doivent remplir toutes les conditions ci-dessous :

- le périmètre d'application de la certification dont dispose l'hébergeur doit inclure le périmètre pour lequel le candidat demande une certification HDS ;
- les rapports d'audit : le rapport d'audit initial et les rapports d'audit de surveillance de la certification dont l'équivalence est demandée doivent être fournis sur demande de l'organisme de certification ;
- pour un candidat disposant d'une certification ISO 27001, la déclaration d'applicabilité (DdA) du système de gestion de la sécurité des informations de l'organisation doit expressément inclure :
    - la justification détaillée de toute exclusion de contrôles de l'ISO 27001 ;
    - la justification détaillée de tout contrôle non applicable ;

- les certifications doivent :
  - être en cours de validité ;
  - avoir été délivrées par un organisme de certification accrédité par une instance nationale d'accréditation telle que définie dans le règlement (CE) n° 765/2008[6] pour la délivrance de ces certificats et dont l'accréditation doit être en cours de validité (le COFRAC en France ou son équivalent dans les autres pays signataires des accords multilatéraux de reconnaissance internationaux) ;
  - ne pas faire l'objet d'une procédure de suspension ou de retrait ;
  - ne pas faire l'objet d'une demande de transfert.

Les conditions ci-dessus doivent faire l'objet d'une vérification par l'organisme de certification recevant la demande de certification HDS, qui doit enregistrer les informations reçues (copies des certificats notamment) et justifier les résultats de cette vérification en indiquant quelle(s) certification(s) est (sont) acceptée(s) par l'OC préalablement à l'audit initial du candidat.

Les certifications obtenues selon des normes internationales équivalentes aux normes françaises indiquées ci-dessus pourront être reconnues selon les mêmes conditions.

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:FR:PDF

Annexe A : Tableau de durée d'audit pour la certification HDS

Le tableau de temps d'audit ci-dessous fournit le cadre qui doit être utilisé pour la planification de l'audit de certification HDS en identifiant un point de départ basé sur le nombre total de personnes travaillant sous le contrôle de l'organisation pour tous les postes impliqués dans le service d'hébergement de données de santé et en ajustant les facteurs importants.

L'OC doit fournir la détermination du temps d'audit et les justificatifs au client. Ceux-ci font partie intégrante du contrat et doivent être tenus à disposition de l'organisme d'accréditation sur demande.

Le point de départ pour déterminer le temps d'audit d'une certification HDS doit reposer sur le nombre réel d'employés impliqués dans le service d'hébergement de données de santé, puis pourra être ajusté en fonction de facteurs significatifs s'appliquant au client à auditer.

	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
Nombre de personnes impliquées dans le service d'hébergement de données de santé	(A) Durée d'audit NF ISO 27001	(B) Durée d'audit des exigences hors NF ISO 27001	Durée totale de l'audit de certification HDS
1 - 10	5	1	6
11 - 15	6	1	7
16 - 25	7	1,5	8,5
26 - 45	8,5	2	10,5
46 - 65	10	2	12
66 - 85	11	2	13
86 - 125	12	2,5	14,5
126 - 175	13	2,5	15,5
176 - 275	14	3	17
276 - 425	15	3	18
426 - 625	16,5	3,5	20
626 - 875	17,5	3,5	21
876 - 1175	18,5	4	22,5
1176 - 1550	19,5	4	23,5
1551 - 2025	21	4	25
2026 - 2675	22	4,5	26,5
2676 - 3450	23	4,5	27,5

	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
Nombre de personnes impliquées dans le service d'hébergement de données de santé	(A) Durée d'audit NF ISO 27001	(B) Durée d'audit des exigences hors NF ISO 27001	Durée totale de l'audit de certification HDS
3451 - 4350	24	5	29
4351 - 5450	25	5	30
5451 - 6800	26	5	31
6801 - 8500	27	5,5	32,5
8501 - 10700	28	5,5	33,5
> 10700	Suivre la progression ci-dessus	Suivre la progression ci-dessus	Suivre la progression ci-dessus

La durée d'audit pourra être ajustée à la hausse ou à la baisse en fonction de facteurs spécifiques selon les bonnes pratiques en vigueur. Ces facteurs pourront être, à titre d'exemple, la complexité de l'environnement à auditer, les contraintes logistiques liées à l'audit, ou la connaissance préalable du contexte.

Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente

Rapport annuel HDS

Nom de l'organisme de certification : *XXXX*

Date : *jj/mm/aaaa*

Synthèse des certifications HDS, des audits réalisés et des non-conformités relevées

Synthèse des difficultés rencontrées lors de la certification HDS

Propositions d'amélioration de la certification HDS

Indicateurs sur la procédure de certification HDS

Nombre de certifiés "hébergeur d'infrastructure physique" **(A)**	Nombre de certifiés "hébergeur infogéreur" **(B)**	Nombre de certifications délivrées **(A+B)**	Nombre d'échecs	Nombre de renouvellements	Nombre de suspensions	Nombre de retraits	Nombre de certifications transférées
XXXX	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*

Annexe C : Notification de suspension de certification

Rapport de suspension HDS

Nom de l'organisme de certification : *XXXX*

Date : *jj/mm/aaaa*

Nom hébergeur de données de santé	*XXXX*
Numéro d'identifiant du certificat	*No. XXXX*
Date de suspension	*jj/mm/aaaa*
Raisons de la suspension	*XXXX*

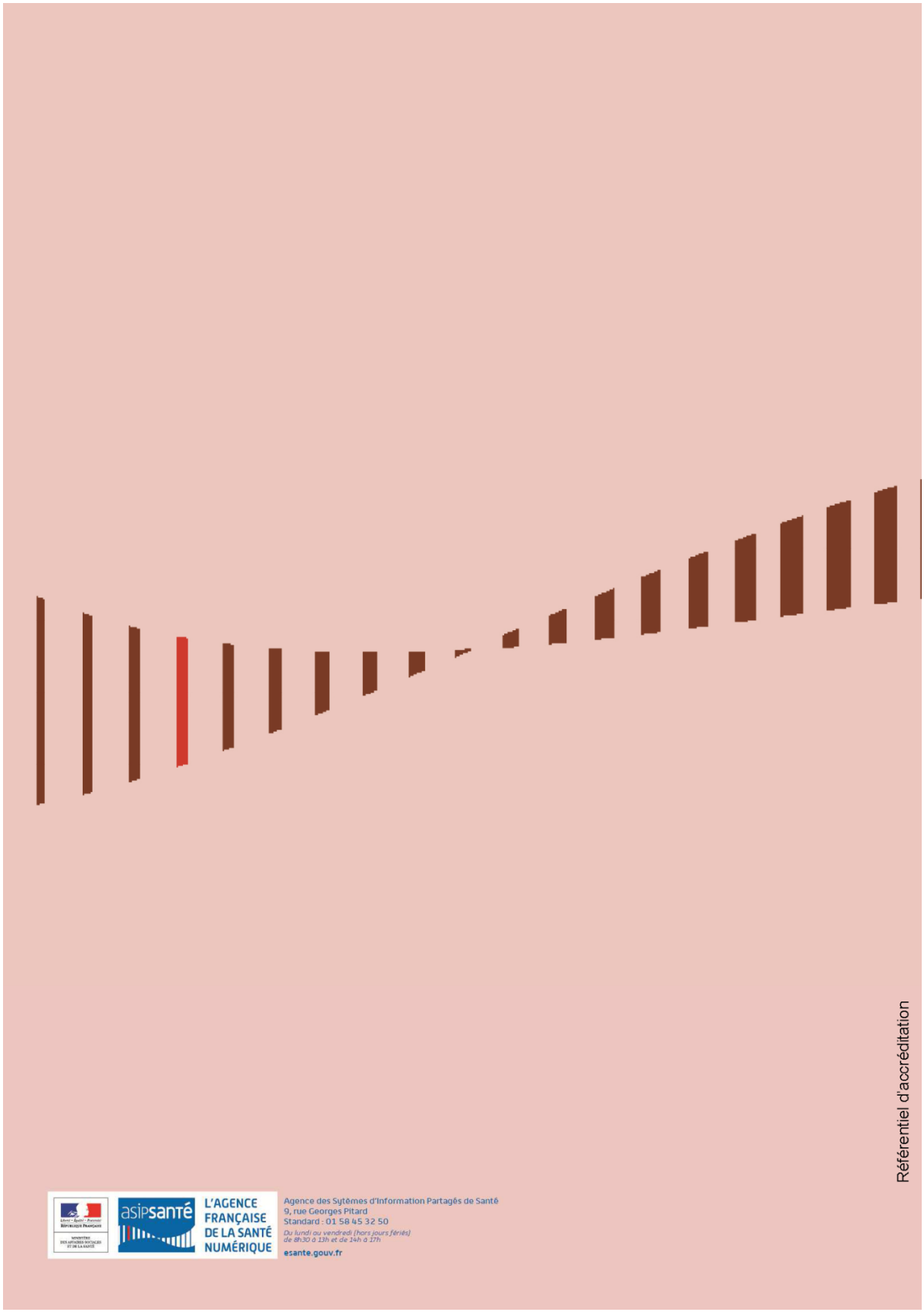
Annexe D : Notification de retrait de certification

Rapport de retrait HDS

Nom de l'organisme de certification : *XXXX*

Date : *jj/mm/aaaa*

Nom hébergeur de données de santé	*XXXX*
Numéro d'identifiant du certificat	*No. XXXX*
Date de retrait	*jj/mm/aaaa*
Raisons du retrait	*XXXX*


Référentiel d'accréditation
asipsanté
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