AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici



Référentiel d'accréditation HDS

Statut : Validé | *Classification : Public* | *Version : ~~v2.0~~v2.1*

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Documents de référence

Référence n°1 : NF EN ISO/IEC 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 EN ISO/IEC 27001:2023~~2~~

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information Exigences

Référence n°3 : Référentiel de certification HDS exigences v2.~~0~~ 1

Référence n°4 : IAF MD1 version en vigueur

Document d'exigences IAF pour la certification multi sites par échantillonnage

Référence n°5 : IAF MD2 version en vigueur

Document d'exigences IAF pour le transfert d'une certification sous accréditation de systèmes de management

Référence n°6 : IAF MD4 version en vigueur

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°7 : IAF MD5 version en vigueur

Détermination du temps d'audit des systèmes de management de la qualité et des systèmes de management environnemental

Référence n°8 : IAF MD11 version en vigueur

Document d'exigences IAF pour l'application de la norme ISO/IEC 17021 pour les audits de Systèmes de Management Intégrés (SMI)

Les documents d'exigences IAF sont disponibles sur le site de l'IAF.

SOMMAIRE

1. INTRODUCTION 3
1.1. Objet du document 3
1.2. Structure du document 3
1.2.1. Définitions 3
2. CHAMP D'APPLICATION 5
2.1. Applicabilité du référentiel de certification HDS 5
2.1.1. Rôle d'Hébergeur 5
2.1.2. Nature des données 5
2.1.3. Contexte du recueil 5
2.1.4. Activités réalisées 5
3. RÉFÉRENCES NORMATIVES 7
4. ACRONYMES UTILISÉS 8
5. CONDITIONS, CRITÈRES ET MODALITÉS D'ACCRÉDITATION 9
5.1. Conditions et critères d'accréditation 9
5.2. Exigences d'accréditation 9
5.2.1. Exigences générales 9
5.2.2. Exigences structurelles 10
5.2.3. Exigences relatives aux informations 11
5.2.4. Exigences du processus de certification 13
5.2.5. Modalités d'évaluation 15
6. RESPONSABILITÉS DES ORGANISMES D'ACCRÉDITATION 16
6.1. Processus d'accréditation 16
6.2. Processus de suspension de l'accréditation 17
6.2.1. Décision de suspension 17
6.2.2. Levée de suspension 17
6.3. Processus de retrait de l'accréditation 17
6.4. Transfert de certification à un nouvel organisme de certification à la suite d'un retrait 18
6.5. Cessation d'activité d'un organisme de certification 18
7. CONDITIONS, CRITÈRES ET MODALITÉS DE CERTIFICATION 19
7.1. Conditions et critères de certification 19
7.2. Equivalence 19
7.3. Sous traitance 20
ANNEXE A : TABLEAU DE DUREE D'AUDIT POUR LA CERTIFICATION HDS 21
ANNEXE B : ECHANGES D'INFORMATIONS ENTRE L'ORGANISME DE CERTIFICATION ET L'AUTORITE COMPETENTE 230

1. INTRODUCTION

1.1. Objet du document

Ce document s'adresse aux organismes de certification souhaitant être accrédités pour la certification des Hébergeurs de données de santé. 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 deux annexes :

- introduction du document ;
- description du champ d'application du référentiel d'accréditation ;
- description des normes applicables au sein du référentiel d'accréditation ;
- liste des acronymes utilisés dans le référentiel d'accréditation ;
- description des conditions, critères et modalités d'accréditation des organismes de certification ;
- définition des responsabilités des organismes d'accréditation ;
- description des conditions, critères et modalités de certification des Hébergeurs.

Annexes

- annexe A présentant les éléments nécessaires permettant de déterminer la durée d'audit pour la certification HDS ;
- annexe B présentant les modèles de documents à utiliser par les organismes de certification pour envoyer des informations à l'autorité compétente.

1.2.1. Définitions

1.2.1.1. Acteur

Tout intervenant contribuant à la sécurité des données de santé à caractère personnel, à l'exclusion du responsable de traitement et des sous-traitants d'un Hébergeur certifié lorsqu'ils agissent conformément à la politique de sécurité et sous la surveillance dudit Hébergeur

1.2.1.2. Administration et exploitation du système d'information contenant les données de santé

L'activité d'administration et exploitation du système d'information contenant les données de santé consiste en la maitrise des interventions sur les ressources mises à la disposition du client de l'Hébergeur. Elle comprend l'intégralité des activités annexes suivantes :

- la définition d'un processus d'attribution et de revue annuelle de droits d'accès nominatifs, justifiés et nécessaires;

- la sécurisation de la procédure d'accès ;
- la collecte et la conservation des traces des accès effectués et de leurs motifs ;
- la validation préalable des interventions (plan d'intervention, processus d'intervention).

La validation des interventions consiste à s'assurer qu'elles ne dégradent la sécurité de l'information hébergée ni pour le client concerné ni pour les autres clients de l'Hébergeur. Cette validation peut être effectuée dans les cas suivants :

- a priori, pour les interventions que le client pourrait effectuer en autonomie ;
- lors de la demande d'intervention lorsqu'il sollicite l'Hébergeur.

La définition du processus d'attribution, la sécurisation, la collecte, la validation sont intrinsèques et obligatoires aux activités définies au 1 à 4 de l'article R. 1111-9 du code de la santé publique. Si elles sont effectuées uniquement en ce qu'elles sont liées et consubstantielle aux activités 1 à 4, l'Hébergeur n'est pas tenu d'être certifié pour l'activité 5. Il ne sera tenu de l'être que dans le cas où il exerce uniquement l'activité 5.

1.2.1.3. Client de l'Hébergeur

Le client de l'Hébergeur (également dénommé « client ») désigne la personne physique ou morale souscrivant au service mis en œuvre par l'Hébergeur.

1.2.1.4. Hébergeur

L'Hébergeur, également désigné organisation dans la norme ISO 27001, est le candidat à la certification des Hébergeurs de données de santé ou au renouvellement de sa certification. Il fournit tout ou partie d'un service d'hébergement de données de santé à caractère personnel (ou « données de santé »).

1.2.1.5. Moyen d'identification électronique

Un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier à un service en ligne.

1.2.1.6. Responsable de traitement

Le responsable de traitement au sens du règlement n°2016/679 désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

2. CHAMP D'APPLICATION

2.1. Applicabilité du référentiel de certification HDS

Le champ d'application du référentiel est défini par les articles L. 1111-8, R. 1111-8-8 et R. 1111-9 du code de la santé publique.

2.1.1. Rôle d'Hébergeur

La certification HDS s'applique à toute personne physique ou morale qui fournit tout ou partie d'un service d'hébergement de données de santé à caractère personnel et qui a la qualité de sous-traitant au sens de l'article 28 du RGPD.

2.1.2. Nature des données

Les données hébergées doivent être des données à caractère personnel concernant la santé, telles que définies à l'article 4.15 du RGPD.

2.1.3. Contexte du recueil

Sont concernées par la certification HDS, les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social. Ces données de santé à caractère personnel doivent être hébergées pour le compte :

- des personnes physiques ou morales à l'origine de la production ou du recueil des données ;
- ou du patient lui-même.

2.1.4. Activités réalisées

L'article R. 1111-9 du CSP définit l'activité d'hébergement de données de santé.

Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

1° La mise à disposition et le maintien en condition opérationnelle de 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 l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;

4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

5° L'administration et l'exploitation du système d'information contenant les données de santé ;

6° La sauvegarde des données de santé, notamment leur conservation dans le cadre d'un archivage électronique.

L'activité 5 est précisée au paragraphe 1.2.1.2.

L'activité 6 de sauvegarde des données, notamment leur conservation dans le cadre d'un archivage électronique, doit être interprétée comme comprenant uniquement les sauvegardes externalisées. Les sauvegardes intrinsèquement nécessaires aux activités 1 à 5 sont dans le périmètre des activités 1 à 5.

3. RÉFÉRENCES NORMATIVES

Les documents, listés ci-dessous sont référencés de manière normative dans le présent référentiel et sont indispensables pour son application.

NF EN ISO 27001:2023, *Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences*

NF EN ISO/IEC 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 EN ISO 27001:2023 ;
- NF ISO 17021 1 pour la norme NF EN 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 / IEC	Commission Electrotechnique Internationale / International Electronical Commission
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 être accrédité selon les exigences de 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 selon la norme ISO 27001. 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 :

- de sélectionner des auditeurs et des experts techniques sur la base de leurs compétences, leurs formations, leurs qualifications et leur expérience ;
- 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

Nota bene

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 « Champ d'application », notamment la liste des activités certifiées;
- spécifier les normes ISO pour lesquelles l'organisme est déjà certifié et dont il respecte les exigences en vigueur (NF ISO 27001).
- préciser la localisation (a minima le pays) de tous les sites entrant dans le périmètre de certification.

Lorsqu'une certification ISO 27001 est délivrée par un OC différent de celui qui délivre la certification HDS, le certificat doit comporter une mention explicite indiquant qu'il est valable sous condition d'obtention d'une certification ISO 27001 valide pour le même périmètre.

Nota bene

En cas de recours à des sous-traitants, les sites de ces derniers ne figurent pas sur le certificat.

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.

5.2.3.5. Echanges d'informations avec l'autorité compétente

5.2.3.5.1. 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.

5.2.3.5.2. 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

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.

5.2.3.5.3. Répertoire clients HDS

L'organisme de certification doit fournir, a minima une fois par mois, 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 ;
- périmètre de la certification (liste des activités) ;

- 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.
- URL ou contact afin de permettre la vérification du certificat auprès de l'OC.
- URL de la page de déclaration des transferts des DSCP conformément à l'exigence 31 du référentiel de 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.

5.2.3.5.4. 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

5.2.4.1.1. 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 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.

5.2.4.1.2. Revue de la demande

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

5.2.4.1.3. Programme d'audit

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

Le chapitre 9.1.3.1 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.

5.2.4.1.4. 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 et MD 5 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).

5.2.4.1.5. Echantillonnage multiple

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

5.2.4.1.6. 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.

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.

5.2.4.4. Réalisation des audits

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

Des représentants de l'Agence du Numérique en Santé peuvent assister en tant qu'observateurs à la réalisation d'un audit.

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

5.2.4.10.1. Options

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

5.2.4.10.2. 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.

5.2.4.10.3. 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 douze (12) mois.

L'accréditation doit être obtenue dans un délai maximum de douze (12) 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 douze (12) 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	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 (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 en précisant : le nom de l'organisme de certification, la date de suspension, les motivations de la décision de suspension et la date à laquelle l'accréditation sera retirée si les conditions de levée de la suspension ne sont pas respectées.

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.

L'envoi de la notification de levée de suspension à l'autorité compétente doit être réalisé par voie électronique en précisant : le nom de l'organisme de certification, la date de suspension (le cas échéant), les motivations de la décision de suspension et la date de levée de la suspension.

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 précisant : le nom de l'organisme de certification, la date de suspension (le cas échéant), les motivations de la décision de retrait de l'accréditation et la date à laquelle l'accréditation a été retirée.

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. En particulier, le guide IAF MD2 s'applique. 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.

La certification d'un Hébergeur nécessite :

- qu'il ait mis en œuvre un Système de Management de la Sécurité de l'Information (SMSI) certifié selon la norme ISO 27001, complétée des exigences définies au chapitre 5 du référentiel de certification ;
- que le domaine d'application de ce SMSI couvre l'ensemble des activités d'hébergement de données de santé de l'Hébergeur ;
- que les contrats conclus avec ses clients répondent aux exigences définies au chapitre 6 du référentiel de certification ;
- qu'il respecte les exigences relatives à la souveraineté définies au chapitre 7 du référentiel de certification ;
- qu'il communique à ses clients la présentation des garanties formalisée conformément au chapitre 8 du référentiel de certification.

Un Hébergeur qui a déjà obtenu une certification ISO 27001 peut faire prévaloir cette certification s'il remplit les conditions citées dans le chapitre 7.2.

Un candidat disposant déjà de cette certification est évalué sur le périmètre des exigences du référentiel de certification non couvertes par la certification. La certification déjà obtenue fait l'objet d'une vérification selon les modalités définies au chapitre 7.2.

Le certificat HDS est délivré pour 3 ans : la date de fin de validité peut être différente de la date de fin de validité du certificat ISO 27001.

Le certificat HDS comporte une mention explicite indiquant qu'il est valable sous condition d'une certification ISO 27001 valide pour le même périmètre.

Dans le contrat entre l'OC et son client, les mentions suivantes doivent apparaitre :

- Le client est informé qu'en cas de non conformité relative à une exigence de l'ISO 27001 constatée à l'occasion d'un audit HDS, cette information est transmise à l'OC qui a certifié le client selon l'ISO 27001.
- Le client a l'obligation d'informer immédiatement l'OC de toute mesure de suspension, retrait, résiliation ou transfert de son certificat ISO 27001.

Ces engagements font l'objet d'une vérification lors des audits de surveillance.

7.2. Equivalence

Si le candidat souhaite faire prévaloir la certification selon la norme NF ISO 27001 qu'il a déjà obtenue, cette certification doit 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 ;
- la certification doit :
- être en cours de validité ;
- avoir été délivrée par un organisme de certification accrédité par une instance nationale d'accréditation telle que définie dans le règlement (CE) n° 765/2008 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. Il s'agit notamment des certifications de conformité aux normes ISO 27001 et ISO 17021 dans d'autres langues que le français.

7.3. Sous-traitance

En cas de recours à des sous-traitants par l'Hébergeur, la représentation des garanties décrite au chapitre 8 du référentiel de certification HD s'applique.

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.

Nombre de personnes impliquées dans le service d'hébergement de données de santé	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
	(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
0			0,5[1]
1 – 10	5	2	7
11 - 15	6	2	8
16 - 25	7	2	9
26 - 45	8,5	2	10,5
46 - 65	10	3	13
66 - 85	11	3	14
86 - 125	12	3	15
126 - 175	13	3	16
176 - 275	14	3	17
276 - 425	15	3	18
426 - 625	16,5	4	20,5
626 - 875	17,5	4	21,5
876 - 1175	18,5	4	22,5
1176 - 1550	19,5	4	23,5
1551 – 2025	21	4	25
2026 – 2675	22	4	26

[1] Aucun facteur de réduction ne peut s'appliquer sur cette ligne

Nombre de personnes impliquées dans le service d'hébergement de données de santé	Durée d'audit de la certification HDS (étape 1 + étape 2) A+B		
	(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
2676 – 3450	23	4	27
3451 – 4350	24	5	29
4351 – 5450	25	5	30
5451 – 6800	26	5	31
6801 – 8500	27	5	32
8501 - 10700	28	5	33
10701	Suivre la progression ci-dessus	Suivre la progression ci-dessus	Suivre la progression ci-dessus

La durée d'audit HDS pourra être ajustée à la hausse ou à la baisse en fonction de facteurs spécifiques selon les bonnes pratiques en vigueur pour le calcul des durées d'audit d'un SMSI. Ces facteurs sont la complexité du SMSI, la nature du service concerné, la preuve d'une mise en œuvre préalable d'un SMSI, la complexité technologique mise en œuvre, le recours à des sous-traitants, la nature des développements éventuels et le nombre de sites. Les modifications apportées au SMSI sont un facteur à prendre en compte pour le calcul des durées des audits de surveillance et de recertification.

Selon les règles de bonnes pratiques en vigueur pour le calcul des durées d'audit d'un SMSI, la réduction maximale de la durée d'audit est de 30%, l'augmentation maximale de la durée d'audit est de 100%. Ces limites s'appliquent au calcul de la durée d'audit HDS.

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

Rapport annuel HDS	
Nom de l'organisme de certification : XXX	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 certifications délivrées	Nombre d'échecs	Nombre de renouvellements	Nombre de suspensions	Nombre de retraits	Nombre de certifications transférées

Répertoire clients HDS

Nom de l'organisme de certification : XXX

Date : jj/mm/aaaa

Identifiant du certificat	Nom Hébergeur de données de santé	Périmètre de la certification (liste des activités)	URL de la page de déclaration des risques de transfert des DSCP conformément à l'exigence 31	Adresse des sites	Date de certification	Etat du certificat	URL de publication du certificat ou contact OC