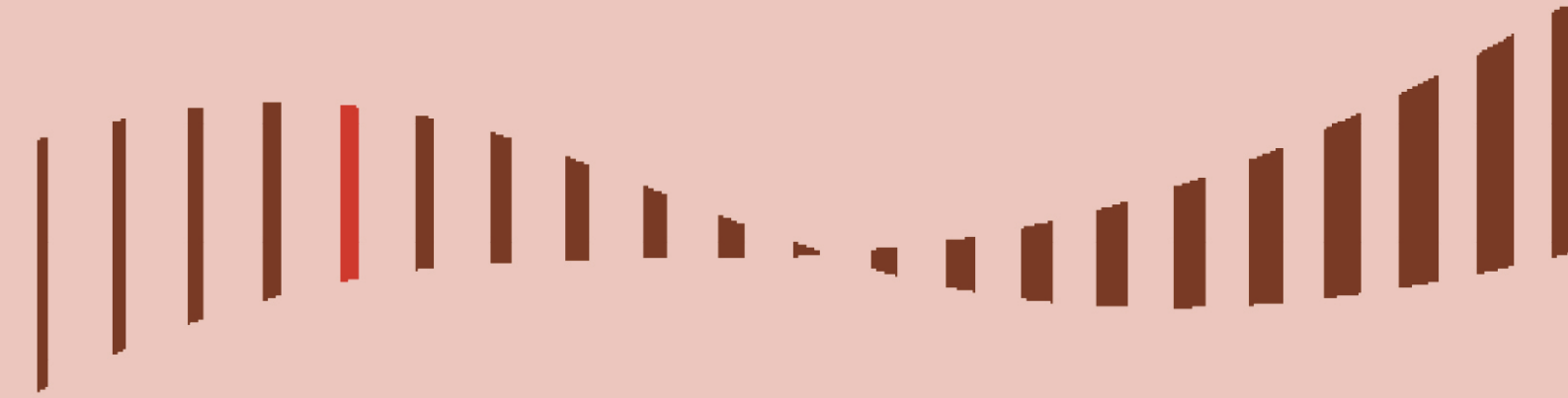
V 1.1

REFERENTIEL DE CERTIFICATION HDS

Exigences et contrôles

Version 1.1 – Juin 2018



asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

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.

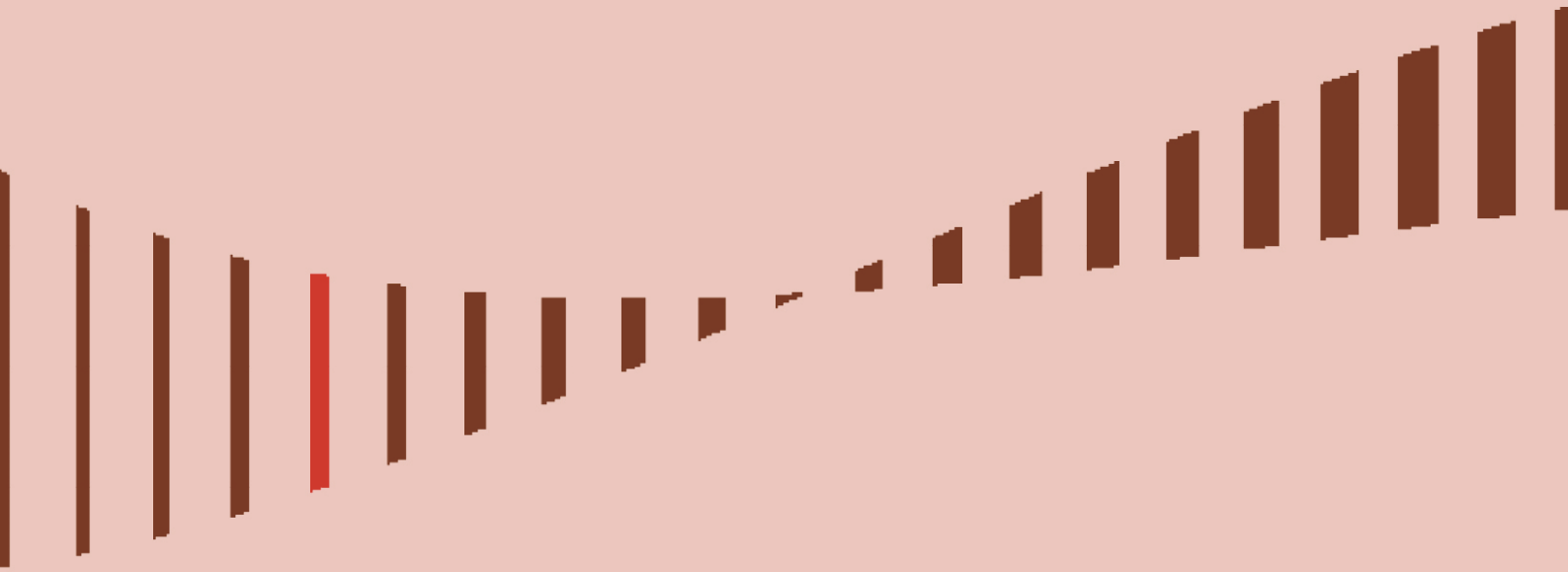
4.5.5. Régionalisation

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.



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