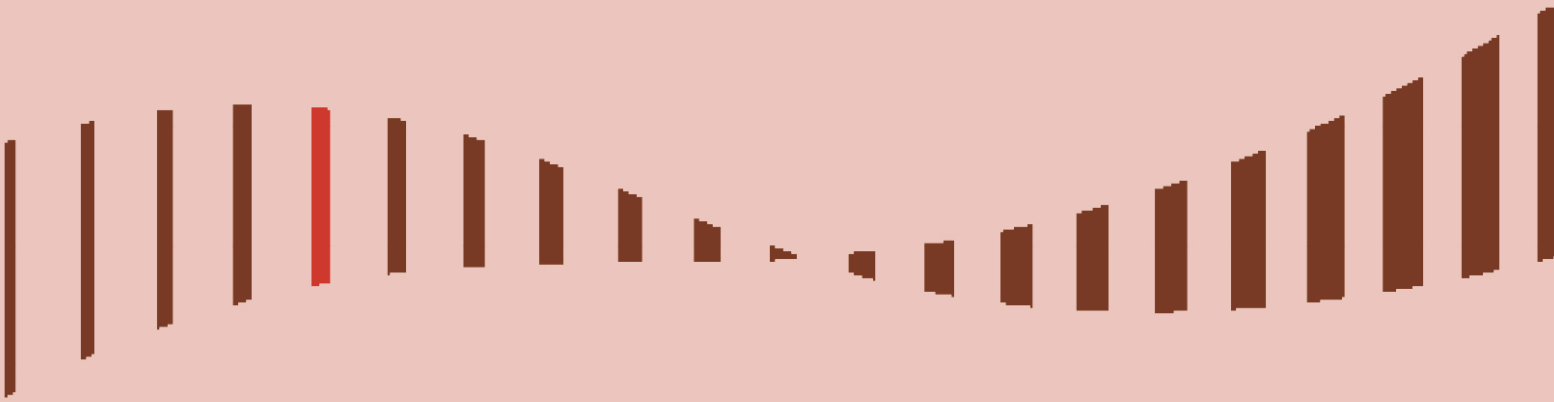
V 1.0

REFERENTIEL DE CERTIFICATION HDS

Exigences et contrôles

Version 1.0 – Novembre 2017



asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Documents de référence

Référence n°1 : ISO/IEC 27001:2013
Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences

Référence n°2 : 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

Référence n°3 : ISO/IEC 27017:2015
Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Référence n°4 : ISO/IEC 20000-1:2011
Technologies de l'information – Gestion des services – Partie 1 Exigences du système de management des services

Référence n°5: Référentiel d'accréditation HDS

Sommaire

1. Introduction 4
1.1. Objet du document 4
1.2. Structure du document 4
2. Références normatives 5
3. Termes et définitions 6
4. Exigences du référentiel de certification HDS 7
4.1. Liens entre les exigences et les normes 7
4.2. Exigences ISO/IEC 27001:2013 7
4.3. Exigences ISO/IEC 20000-1:2011 8
4.3.1. Planification de nouveaux services ou de services modifiés 8
4.3.2. Conception et implémentation des nouveaux services ou des services modifiés 8
4.3.3. Continuité de services et gestion de la disponibilité 9
4.4. Exigences ISO/IEC 27018:2014 9
4.4.1. Consentement et choix 9
4.4.2. Finalité 9
4.4.3. Utilisation, conservation et communication 10
4.4.4. Transparence 10
4.4.5. Responsabilité 10
4.4.6. Sécurité des données 11
4.4.7. Localisation des données 13
4.5. Exigences ISO/IEC 27017:2015 13
4.5.1. Rôles et responsabilités 13
4.6. Exigences complémentaires 13
4.6.1. Conformité aux référentiels opposables de la PGSSI-S 13
4.6.2. Rapports d'audit 14
4.6.3. Liste des contacts clients 14
4.6.4. Régionalisation 14

1.Introduction

1.1. Objet du document

Le présent document constitue le référentiel de certification applicable aux hébergeurs souhaitant obtenir une certification « 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. l'introduction ;

2. la présentation des normes internationales retenues dans le cadre de la certification pour l'hébergement de données de santé à caractère personnel ;

3. la définition des notions utilisées dans le référentiel de HDS ;

4. la liste exhaustive des exigences du référentiel HDS portant sur les deux périmètres de certification « hébergeur d'infrastructure physique » ou « hébergeur infogéreur ».

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

2.Références normatives

La liste des normes applicables dans le cadre de la certification HDS est présentée ci-dessous.

Pour les normes datées, seule l'édition citée s'applique. Pour les normes non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

ISO/IEC 27017:2015, *Technologies de l'information – Techniques de sécurité - Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*

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 :

- ISO 27001 pour la norme ISO/IEC 27001:2013 ;
- ISO 20000-1 pour la norme ISO/IEC 20000-1:2011 ;
- ISO 27017 pour la norme ISO/IEC 27017:2015 ;
- ISO 27018 pour la norme ISO/IEC 27018:2014.

3.Termes et définitions

Pour les besoins du présent document, les termes et définitions suivantes s'appliquent:

CE	Commission Européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
COFRAC	Comité Français d'Accréditation
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
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
Multi-sites	Service d'hébergement réalisé sur plusieurs sites géographiques
OC	Organisme de Certification
PII	Informations Personnelles Identifiables
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 issues de normes existantes et également d'exigences spécifiques au contexte HDS.

Le référentiel HDS comprend ainsi :

- les exigences de la norme ISO 27001 reprise dans son intégralité ;
- une partie des exigences énumérées dans la norme ISO 20000-1 ;
- une partie des objectifs et mesures énumérés dans la norme ISO 27018 généralisés à des services d'hébergement hors Cloud;
- une partie des exigences énumérées dans la norme ISO 27017 généralisées à des services d'hébergement hors Cloud ;
- des exigences spécifiques au domaine de la santé.

4.2. Exigences ISO/IEC 27001:2013

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

En outre, les exigences spécifiques suivantes s'appliquent.

Exigence spécifique complétant le chapitre 4.3 de l'ISO 27001

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'organisation 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'organisation.

Exigence spécifique complétant le chapitre 6.1.3 de l'ISO 27001

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : La DdA (déclaration d'applicabilité) du SMSI doit inclure les exigences du référentiel de certification HDS (i.e. les exigences spécifiques santé, l'annexe A de l'ISO 27001:2013, les exigences ISO 20000-1:2011, les exigences ISO 27018:2014 et l'exigence de l'ISO 27017 énoncés ci-dessous). Toute exclusion d'exigences du périmètre de certification doit être formellement justifiée et la justification doit être approuvée par l'organisme de certification.

Exigence spécifique complétant l'Annexe A12.3 de l'ISO 27001

Application : Hébergeurs infogéreurs

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

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 spécifique complétant l'Annexe A12.7 de l'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.)

4.3. Exigences ISO/IEC 20000-1:2011

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

4.3.1. Planification de nouveaux services ou de services modifiés

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

En outre l'exigence spécifique suivante s'applique.

Exigence spécifique complétant le chapitre 5.3 de l'ISO 20000-1

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Des critères d'acceptation du service pour les nouveaux services ou services modifiés, et des tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à 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 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 ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4. Exigences ISO/IEC 27018:2014

Les exigences de la norme ISO 27018 sont des recommandations orientées sur la protection de données à caractère personnel dans le cadre d'hébergement de type « Cloud ».

Les exigences identifiées[2] dans le cadre de l'obtention de la certification HDS sont **d'application obligatoire** et **étendues aux activités d'hébergement hors Cloud.**

4.4.1. Consentement et choix

4.4.1.1. Obligation de coopérer

L'Annexe A 1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.2. Finalité

L'Annexe A 2.1 de la norme ISO 27018 s'applique aux d'infrastructure physique et aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante s'applique.

[2] Les exigences de la norme ISO 27018 identifiées dans le cadre de l'obtention de la certification HDS ne représentent pas la totalité des exigences de la norme

Exigence spécifique complétant l'Annexe A 2.1 de l'ISO 27018

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'hébergeur ne doit pas utiliser les données de santé 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 statistique.

4.4.3. Utilisation, conservation et communication

4.4.3.1. Données temporaires

L'Annexe A.4.1 de la norme ISO 27018 s'applique uniquement aux hébergeurs infogéreurs.

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

L'Annexe A 5.1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.3.3. Traçabilité en cas de communication

L'Annexe A 5.2 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.4. Transparence

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

L'Annexe A 7.1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.5. Responsabilité

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

L'Annexe A 9.1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante s'applique.

Exigence spécifique complétant l'Annexe A 9.1 de l'ISO 27018

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs. Objectif : L'hébergeur doit définir et mettre en œuvre des mesures organisationnelles et techniques afin d'assister son client en cas d'incident de sécurité ayant une cause accidentelle pouvant provoquer une altération, divulgation ou perte d'intégrité de l'information.

4.4.5.2. Période de conservation des politiques de sécurité

L'Annexe A 9.2 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.5.3. Gestion des informations personnelles

L'Annexe A 9.3 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

Exigence spécifique complétant l'Annexe A 9.3 de l'ISO 27018

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

L'Annexe A 10.1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.2. Restriction de copie matérielle

L'Annexe A 10.2 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.3. Contrôle et traçabilité lors de la restauration de données

L'Annexe A 10.3 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

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

L'Annexe A 10.4 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.5. Utilisation de support de stockage portable

L'Annexe A 10.5 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.6. Chiffrement des données personnelles transmises sur des réseaux publics

L'Annexe A 10.6 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.7. Destruction des copies matérielles

L'Annexe A 10.7 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.8. Utilisation d'identifiants uniques

L'Annexe A 10.8 de la norme ISO 27018 s'applique uniquement aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante s'applique.

Exigence spécifique complétant l'annexe A 10.8 de l'ISO 27018

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

4.4.6.9. Gestion des habilitations

L'Annexe A 10.9 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.10. Gestion des traces

Le chapitre 12.4 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante s'applique.

Exigence spécifique complétant le chapitre 12.4 de l'ISO 27018

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

L'Annexe A 10.10 de la norme ISO 27018 s'applique uniquement aux hébergeurs infogéreurs.

4.4.6.12. Clauses contractuelles

L'Annexe A 10.11 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.13. Sous-traitance du traitement des données personnelles

L'Annexe A 10.12 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.6.14. Réutilisation des espaces de stockage

L'Annexe A 10.13 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.4.7. Localisation des données

4.4.7.1. Lieux d'hébergement

L'Annexe A 11.1 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

En outre l'exigence spécifique suivante s'applique.

Exigence spécifique complétant l'Annexe A 11.1 de l'ISO 27018

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : L'hébergeur doit informer le 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.

4.4.7.2. Transfert des données

L'Annexe A 11.2 de la norme ISO 27018 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs.

4.5. Exigences ISO/IEC 27017:2015

4.5.1. Rôles et responsabilités

Dans le cadre de la certification des hébergeurs de données de santé à caractère personnel, l'exigence de la partie 6.1.1 de l'ISO 27017 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs et est **étendue aux activités d'hébergement hors Cloud**.

4.6. Exigences complémentaires

4.6.1. 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 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.

4.6.2. 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.

4.6.3. Liste des contacts clients

Application : Hébergeurs d'infrastructure physique et hébergeurs infogéreurs.

Objectif : Une liste des points de contact pour chacun des clients doit être maintenue par l'hébergeur.

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.

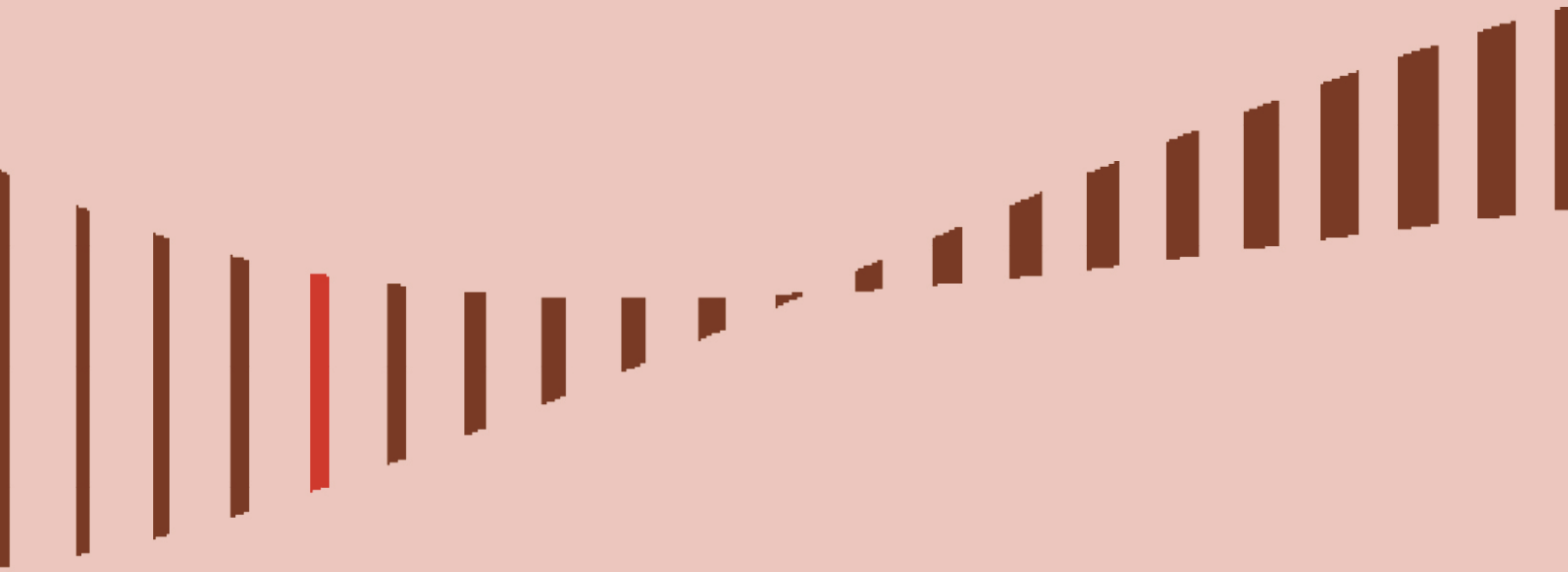
4.6.4. Régionalisation

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 doit être 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