AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Agrément des Hébergeurs de données de Santé

Exemple d'Audit de conformité Sécurité et Technique

« ASIP Santé »

EXEMPLE

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. + 33 (0)1 58 45 32 50
www.asipsante.fr
Agir ensemble pour soigner mieux

Sommaire

1 Glossaire et abréviations 3
1.1 Glossaire 3
1.2 Abréviations 3
2 Liminaire 4
3 Contenu du scénario d'audit 6
4 Analyse détaillée des descriptions des dispositions de sécurité 7
4.1 Politique de Sécurité 7
4.2 Organisation 9
4.3 Gestion des droits des personnes 9
4.4 Ressources humaines 10
4.5 Contrôle d'accès 10
4.6 Télécommunications 11
4.7 Traçabilité 12
4.8 Gestion des incidents 13
4.9 Sauvegarde 13
4.10 Continuité de service 14
4.11 Gestion des évolutions 14
4.12 Conformité 15

EXEMPLE

1 Glossaire et abréviations

1.1 Glossaire

Définitions	
Report	Exigence du décret hébergeur que l'hébergeur reporte contractuellement sur ses clients ou sur ses sous-traitants

1.2 Abréviations

Abréviations	
RDPC	Respect des droits des personnes concernées par les données
SAI	Sécurité de l'accès aux informations
PDH	Pérennité des données hébergées
OPCI	Organisation et procédures de contrôles internes

EXEMPLE

2 Liminaire

En cas de demande de renouvellement de son agrément, l'hébergeur doit adresser un dossier devant contenir les informations financières mises à jour, les moyens mis en œuvre pour prendre en compte les recommandations émises par le ministre en charge de la santé au moment de l'agrément initial, la liste des modifications intervenues depuis la dernière demande d'agrément et les résultats d'un audit externe.

Cet audit externe est réalisé aux frais de l'hébergeur et doit attester de la mise en œuvre de la politique de confidentialité et de sécurité mentionnée à l'article R 1111-14 du code de la santé publique.

Le prestataire d'audit est au libre choix de l'hébergeur, qui pourra utilement se référer au référentiel de qualification publié par l'ANSSI, notamment dans ses volets audit d'architecture, audit de configuration et audit organisationnel et physique.
http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html

Le périmètre de l'audit doit couvrir :

- la conformité des moyens mis en œuvre par l'hébergeur au regard de son dossier d'agrément et des rapports d'auto-évaluation subséquents ;
- la conformité des moyens mis en œuvre au regard des exigences du décret, en tenant compte des évolutions réglementaires et de l'état de l'art depuis son dossier initial ;
- la prise en compte des éventuelles recommandations qui lui auraient été notifiées lors de son agrément initial et des rapports d'auto-évaluation.

Conformité des moyens aux éléments du dossier d'agrément :
L'audit doit vérifier que les moyens techniques, les processus pour garantir la sécurité et confidentialité des données de santé et les reports contractuels de certaines exigences sur le client ou d'éventuels sous-traitants, présentés dans le dossier de demande d'agrément initial et les rapports d'auto évaluation, sont effectivement mis en œuvre.

Conformité des moyens au regard des exigences du décret et des évolutions de l'état de l'art :
L'audit doit assurer que le dossier de demande de renouvellement reste conforme aux exigences du décret et tient compte des évolutions du cadre juridique et de l'état de l'art intervenues depuis son agrément initial.

Prise en compte des recommandations :
L'audit doit également prendre en compte les recommandations majeures qui accompagnaient la décision d'agrément et indiquer ce qui a ou non été mis en place par l'hébergeur pour les respecter.

Les recommandations émises par le ministre en charge de la santé au moment de l'agrément initial ne sont pas exhaustives et un certain nombre d'autres points d'attention peuvent subsister. Il convient de rappeler aux hébergeurs que le courrier de notification de décision favorable d'agrément précise que les services de l'ASIP Santé (qui assure le secrétariat du CAH et la pré-instruction des dossiers de demande d'agrément pour le compte du CAH) se tiennent à la disposition des candidats pour leur apporter toute information complémentaire. L'ensemble des points d'attention, même mineurs, peuvent donc être transmis à l'hébergeur si celui-ci en fait la demande et ce, dans une perspective d'amélioration de son service.

EXEMPLE

L'audit externe doit vérifier la mise en œuvre des points précités. A titre d'exemples, au travers d'une interview, l'auditeur pourrait vérifier si le médecin hébergeur est impliqué dans la gestion des incidents tel que cela pourrait être décrit dans ses missions ; en visitant le site d'un client de l'hébergeur, l'auditeur pourrait apprécier la mise en œuvre par le client de ses obligations définies dans le contrat d'hébergement.

Les résultats de l'audit permettront à l'hébergeur d'améliorer ses processus, de renforcer son devoir de conseil et de planifier un cycle d'amélioration de son service d'hébergement. Ce cycle d'amélioration doit traiter les remarques relevant de la conformité au dossier ou de la prise en compte des recommandations. Pour celles traitant des évolutions de l'état de l'art l'hébergeur peut soit les intégrer à son plan d'actions, soit présenter avec son dossier de renouvellement un argumentaire explicitant en quoi il les considère comme excessives à ce jour, auquel cas le Comité d'Agrément statuera par l'expression de nouvelles recommandations.

L'audit externe ne doit pas dater de plus de six mois avant le dépôt du dossier de demande derenouvellement.

Afin d'aider les hébergeurs à conduire l'audit externe, l'ASIP Santé propose un exemple de scénario d'audit portant sur la conformité des moyens techniques mis en œuvre par l'hébergeur, aux exigences du décret 2006-6 du 4 janvier 2006.

Ce document constitue un simple canevas qui répertorie les exigences énoncées dans le formulaire P6 et prises en compte par l'hébergeur lui-même.

Si l'auditeur utilise ce modèle, il est tenu de le compléter de l'ensemble des points exposés précédemment.

EXEMPLE

3 Contenu du scénario d'audit

Ce document présente un exemple de scénario d'audit de conformité pour le volet « Sécurité & Technique » des dossiers de demande d'agrément pour l'hébergement de données de santé à caractère personnel.

Le scénario d'audit consiste à évaluer les dispositions mises en œuvre en qualifiant les critères d'évaluation sur chacun des thèmes de l'article R. 1111-14 du code de la santé publique. Ces critères d'évaluation consistent à évaluer unitairement les dispositions de sécurité mises en œuvre chez l'hébergeur suivant les 12 thèmes SSI du formulaire « P6 – Formulaire description dispositions sécurité ». Cet audit permettra de valider la conformité :

- des dispositions de sécurité mises en œuvre en réponse aux exigences du « décret hébergeur » formalisées au travers des formulaires du référentiel des dossiers de demande d'agrément ;
- des dispositions de sécurité mises en œuvre en réponse aux éventuelles recommandations portées à la connaissance de l'hébergeur via le courrier de notification de la décision favorable d'agrément.

EXEMPLE

4 Analyse détaillée des descriptions des dispositions de sécurité

4.1 Politique de Sécurité

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur dispose d'une PSSI									
La PSSI est signée par le RSSI									
La PSSI est signée par la DG									
La PSSI est diffusée au personnel									
La PSSI est réévaluée périodiquement									
L'hébergeur a réalisé une analyse de risque sur le périmètre de l'hébergement									
L'hébergeur met à jour régulièrement son analyse de risque									
La PSSI décrit les mesures mises en œuvre pour assurer la sécurité physique des sites									
Les mesures mises en œuvre pour assurer la sécurité physique des sites sont effectives									
La PSSI décrit les mesures mises en œuvre pour assurer la sécurité des réseaux									
Les mesures mises en œuvre pour assurer la sécurité des réseaux sont effectives									
La PSSI décrit les mesures mises en œuvre pour assurer la sécurité des serveurs									
Les mesures mises en œuvre pour assurer la sécurité des serveurs sont effectives									
La PSSI décrit les mesures mises en œuvre pour assurer la sécurité des postes									

de travail								■	
Les mesures mises en œuvre pour assurer la sécurité des postes de travail sont effectives								■	
L'hébergeur a défini une politique d'habilitation						■		■	
L'hébergeur met en œuvre une politique d'habilitation						■		■	
La politique d'habilitations identifie la gestion des identifiants génériques						■		■	
L'hébergeur assure la gestion des identifiants générique définie dans sa politique d'habilitation						■		■	
La politique d'habilitation prend en compte le cycle de vie des habilitations						■		■	
L'hébergeur a décrit les mesures de contrôle de l'application de la politique d'habilitations						■		■	
L'hébergeur assure le contrôle de la mise en œuvre de sa politique d'habilitation						■		■	
L'hébergeur a défini une politique d'authentification						■		■	
L'hébergeur met en œuvre une politique d'authentification						■		■	
L'hébergeur a décrit les mesures de contrôle de l'application de la politique d'authentification						■		■	
L'hébergeur assure le contrôle de la mise en œuvre de sa politique d'authentification						■		■	
L'hébergeur a défini une politique de traçabilité					■	■		■	
L'hébergeur met en œuvre une politique de traçabilité					■	■		■	
La politique de traçabilité prend en compte la restitution des traces aux personnes concernées par les données					■	■		■	
L'hébergeur a défini une politique de surveillance						■		■	
L'hébergeur met en œuvre une politique de surveillance						■		■	
La politique de surveillance permet de restituer l'historique des accès aux personnes concernées par les données						■		■	
L'hébergeur a décrit les mesures de					■	■		■	

surveillance des accès utilisateurs									
L'hébergeur assure une surveillance des accès utilisateurs									

4.2 Organisation

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini son organisation de la sécurité									
Un médecin hébergeur est présent dans l'organisation									
Le médecin hébergeur est associé aux processus de gestion des incidents									
L'hébergeur dispose d'un plan d'assurance qualité									
L'hébergeur identifie le niveau de mutualisation de son infrastructure vis-à-vis de l'activité d'hébergement de données de santé									

4.3 Gestion des droits des personnes

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini les modalités de recueil du consentement des personnes à l'hébergement de leurs données									
L'hébergeur a mis en place les moyens permettant de garantir que l'accès aux données n'est possible que pour les professionnels de santé pour lesquels les personnes concernées par les données ont fourni leur accord									
L'hébergeur a défini les modalités permettant de répondre aux demandes de rectification des données par les personnes concernées									
L'hébergeur a défini les moyens mis en œuvre pour assurer l'accès aux données par les personnes concernées									

L'hébergeur a défini les modalités de signalement des incidents graves aux personnes concernées									
L'hébergeur a défini les modalités de fourniture des historiques des opérations réalisées sur les données aux personnes concernées									

4.4 Ressources humaines

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a classifié ses intervenants internes selon leurs rôles et privilèges									
L'hébergeur a classifié ses intervenants sous traitants selon leurs rôles et privilèges									
L'hébergeur a défini la qualification de ses intervenants internes									
L'hébergeur a défini la qualification de ses intervenants sous traitants									
L'hébergeur a défini un plan de formation et de sensibilisation à la sécurité des données									
L'hébergeur a défini des mesures d'engagement contractuel pour les intervenants sur l'activité d'hébergement									

4.5 Contrôle d'accès

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur met en œuvre des solutions d'authentification et de contrôle d'accès pour les intervenants sur les systèmes									
La robustesse de ces solutions est de type fort									
L'hébergeur a décrit les mesures mises en œuvre pour assurer l'authentification et le contrôle d'accès des établissements de santé									

L'hébergeur met en œuvre des solutions d'authentification et de contrôle d'accès pour les établissements de santé									
La robustesse de ces solutions est de type fort									
L'hébergeur a décrit les mesures mises en œuvre pour assurer l'authentification et le contrôle d'accès des professionnels de santé									
L'hébergeur met en œuvre des solutions d'authentification et de contrôle d'accès pour les professionnels de santé									
La robustesse de ces solutions est de type fort									
L'hébergeur décrit les mesures mises en œuvre pour assurer l'authentification et le contrôle d'accès des personnes concernées par les données									
L'hébergeur met en œuvre des solutions d'authentification et de contrôle d'accès pour les personnes concernées par les données hébergées									
La robustesse de ces solutions est de type fort									
L'hébergeur met en œuvre des solutions d'authentification et contrôle d'accès pour des utilisateurs autres que ceux cités précédemment									
La robustesse de ces solutions est de type fort									

4.6 Télécommunications

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a cartographié les liens mis en œuvre sur son infrastructure									
Ces liens sont sécurisés									
La cartographie du système présente les moyens mis en œuvre concourant à assurer la pérennité des données									
L'hébergeur met en œuvre des moyens assurant l'intégrité des données									

L'hébergeur met en œuvre des moyens assurant l'acquittement de la réception des informations									

4.7 Traçabilité

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini une politique de traçabilité des opérations réalisées sur les données ainsi que sur les systèmes concourant à l'hébergement de celles-ci									
L'hébergeur a identifié les éléments à tracer concernant l'identification des acteurs et les opérations réalisées									
L'hébergeur a défini le périmètre lié à la surveillance des accès aux données de santé									
Le périmètre lié à la surveillance des accès aux données de santé prend en compte les moyens assurant la pérennité des données de traçabilité									
L'hébergeur assure une traçabilité des opérations réalisées sur les données ainsi que sur les systèmes concourant à l'hébergement de celles-ci									
Les éléments tracés sont pertinents et permettent d'identifier clairement les acteurs et les opérations réalisées									
L'hébergeur assure la sauvegarde des traces concernant les accès aux données de santé									
L'hébergeur assure l'archivage des traces concernant les accès aux données de santé									
L'hébergeur a défini les habilitations nécessaires pour l'accès aux données de traçabilité									
L'hébergeur a défini les moyens techniques permettant aux intervenants d'accéder aux traces									
L'hébergeur a défini les moyens organisationnels permettant aux intervenants d'accéder aux traces									

L'hébergeur a défini les moyens techniques permettant aux personnes concernées d'accéder aux traces									

4.8 Gestion des incidents

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini un processus de surveillance des systèmes									
L'hébergeur assure la surveillance des systèmes									
L'hébergeur a défini le processus de gestion des incidents prenant en compte les alertes liées à l'atteinte à l'intégrité des données de santé									
L'hébergeur a défini le processus de gestion des incidents prenant en compte les alertes liées à l'atteinte à la confidentialité des données de santé									
L'hébergeur a défini les procédures d'alertes et d'escalades									
Les procédures d'alertes et d'escalades sont mises en œuvre									
L'hébergeur a établi une classification des incidents									
L'hébergeur a identifié dans sa classification des incidents les incidents de divulgation et altération des données de santé									

4.9 Sauvegarde

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini un plan de sauvegarde									
L'hébergeur met en œuvre un plan de sauvegarde									
Le plan de sauvegarde mis en œuvre prend en compte la sauvegarde des									

données de santé									
Le plan de sauvegarde décrit les moyens mis en œuvre pour réaliser les sauvegardes									
Le plan de sauvegarde présente les moyens mis en œuvre pour assurer la conservation des supports de sauvegarde									
Le plan de sauvegarde présente les moyens mis en œuvre pour assurer l'externalisation des supports									

4.10 Continuité de service

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini des mesures pour assurer la continuité de service									
L'hébergeur met en œuvre les mesures assurant la continuité de service									
L'hébergeur a défini un plan de secours									
L'hébergeur a défini une cellule de crise									
L'hébergeur a défini un plan de communication									
L'hébergeur a défini un plan de reprise d'activité									

4.11 Gestion des évolutions

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini un processus de gestion des évolutions									
L'hébergeur met en œuvre des moyens garantissant la pérennité des données sur les supports de sauvegarde en cas d'évolution du système									
L'hébergeur met en œuvre des moyens garantissant la pérennité des données en cas d'évolution des systèmes									
L'hébergeur a défini une procédure d'alerte vers la personne à l'origine du									

dépôt des données de santé en cas d'évolution des systèmes					■		■		

4.12 Conformité

	Oui	Non	Report	Commentaire	RDPC	SAI	PDH	OPCI	
L'hébergeur a défini un processus de contrôle de conformité								■	
L'hébergeur a formalisé des mesures pour assurer un(des) plan(s) d'action suite aux contrôles								■	

EXEMPLE