ANNEXE HDS

CONDITIONS PARTICULIÈRES RELATIVES À L'HÉBERGEMENT DES DONNÉES DE SANTÉ (HDS)

Préambule

La présente Annexe a pour objet de définir les conditions particulières relatives à l'hébergement des données de santé (HDS) dans le cadre des services fournis par l'ACMOSS au BENEFICIAIRE au titre de la Convention principale. Le BENEFICIAIRE, en tant qu'entité relevant du secours et de l'urgence éligible aux services RRF de l'ACMOSS, souhaite bénéficier de services d'hébergement de données de santé conformes au référentiel HDS.

ARTICLE 1. Périmètre de certification

*Conformément aux bonnes pratiques en matière de mise en conformité des hébergeurs de données de santé, et dans l'attente de l'obtention formelle de la Certification HDS, l’ACMOSS met en œuvre la phase transitoire dite de "Vérification de Service Rendu (VSR)" dans le respect des exigences de l’article R.1111-8-8 I du Code de la santé publique.
Cette phase transitoire est limitée dans le temps et strictement encadrée afin de tester la faisabilité technique et organisationnelle de la gestion des données de santé.*

*Durant cette phase transitoire, l’ACMOSS met en œuvre les garanties suivantes pour assurer la protection des données de santé :*

* *Application d'un Système de Management de la Sécurité de l'Information (SMSI) aligné sur la norme ISO/IEC 27001:2022.*
* *Limitation du volume des données traitées et documentation de l'objectif de "Vérification de Service Rendu (VSR)" de cette phase.*
* *Conformité aux exigences du Règlement Général sur la Protection des Données (RGPD).*
* *Homologation de sécurité des systèmes d'information conforme à l'Instruction Générale Interministérielle n°901 en application des référentiels de sécurité de l'ANSSI, notamment tels que définis dans le* ***Référentiel Général de Sécurité (RGS) et la Politique de Sécurité des Systèmes d’Information de l’État (PSSIE)****.*

La certification HDS visée concerne les activités suivantes :

HÉBERGEMENT d’infrastructure physique

1.la mise à disposition, le maintien en condition opérationnelle de l’infrastructure matérielle du système d’information utilisé pour le traitement de données de santé

2.la mise à disposition, le maintien en condition opérationnelle des sites physiques permettant d’héberger l’infrastructure matérielle du système d’information utilisé pour le traitement des données de santé

HÉBERGEUR infogéreur

3.la mise à disposition et le maintien en condition opérationnelle de l’infrastructure virtuelle du système d’information 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 externalisée des données de santé

Les activités listées ci-dessus correspondent aux finalités des traitements de données réalisés par L’ACMOSS.

La certification HDS est valable trois (3) ans et sera audité annuellement.

La perte de la Certification HDS entraînera la résiliation du volet HDS de la Convention principale dans les conditions prévues à l’article Fin de la prestation, Restitution et Réversibilité.

ARTICLE 2. Rappels des règles applicables

Les Données personnelles de santé sont des données particulières, au sens de l'article 9 du RGPD, qui du fait de leur forte sensibilité et confidentialité, nécessitent une protection renforcée lorsqu'elles font l'objet d'un traitement automatisé.

Cette protection implique notamment la mise en place d'un niveau élevé de sécurité des infrastructures logicielles et informatiques hébergeant des bases de Données personnelles de santé, adapté à la criticité de ces données et aux risques engendrés par leurs traitements sur les droits et libertés fondamentaux des individus.

Ainsi, lorsqu'il est fait appel à un prestataire d'hébergement externalisé, le BENEFICIAIRE est informé que le cadre législatif de l’activité d’hébergement de données de santé à caractère personnel est fixé l'article L. 1111-8 du code de la santé publique (issu de la loi issue de loi n° 2002-303 du 4 mars 2002 relative aux droits des patients et modifié en dernier lieu par la loi 2016-41 du 26 janvier 2016 de modernisation de notre système de santé), qui dispose que : «

 I.- Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article.

II.- L'HÉBERGEUR de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité. »

ARTICLE 3. Documents contractuels

La présente Annexe fait partie intégrante de la Convention principale. En cas de contradiction entre la présente Annexe et la Convention principale, les dispositions de la présente Annexe relatives à l'hébergement des données de santé (HDS) prévaudront. Les éléments qui ne sont pas abordés dans la présente Annexe seront régis par la Convention principale."

ARTICLE 4. Description des Prestations et services réalisés

L’ensemble des prestations délivrées au titre des présentes conditions particulières précisent le cadre de l’hébergement de données de santé en complément de la Convention principale de services ACMOSS.

L’ACMOSS s’engage à garantir la disponibilité, l’intégrité, la confidentialité et l’auditabilité des données hébergées.

ARTICLE 5. Localisation des données

L’Infrastructure de l’ACMOSS supportant la Plateforme de Stockage des Données de Santé est toujours installée dans des datacenters certifiés ISO/CEI  27001 : 2013 et situés en France Métropolitaine.

ARTICLE 6. Recours à des tiers

Dans le cadre des Prestations, le BENEFICIAIRE est informé que L’ACMOSS fait appel aux prestataires externes suivants :

|  |  |  |
| --- | --- | --- |
| **Tiers** | **Adresse** | **Prestations sous-traitées** |
| STIG  | Site de Rosny :1 Boulevard Théophile Sueur93110 ROSNY SOUS BOIS  | Data CENTER(Site production) |
| STIG  | Site de Nogent :1 rue de la Libération 94120 NOGENT SUR MARNE | Data CENTER(Site production) |

Le BENEFICIAIRE autorise l’ACMOSS à faire intervenir ces prestataires dans le cadre de la fourniture des Services.

L’ACMOSS s’assure que ces prestataires présentent un niveau de protection équivalent de garantie au regard des obligations pesant sur l’ACMOSS.

L’ACMOSS peut remplacer un ou plusieurs des prestataires ci-dessus ou recourir à un nouveau prestataire sous réserve de notifier préalablement le BENEFICIAIRE en respectant un délai raisonnable.

L’ACMOSS s’assure que les changements de prestataires ne conduisent pas à une réduction du niveau de sécurité sauf accord préalable du BENEFICIAIRE.

ARTICLE 7. Prestations à la fin de l’hébergement, Restitution et Réversibilité des données de santé

A la fin de l’hébergement, pour quelque raison que ce soit, et notamment dans le cas de perte ou de retrait de la Certification HDS, L’ACMOSS s’engage à permettre la restitution de la totalité des données de santé du BENEFICIAIRE et la réversibilité des prestations d’hébergement HDS conformément au présent article.

La Réversibilité consiste à permettre au BENEFICIAIRE de récupérer toutes les Données de Santé issues de ses communications en vue de les héberger chez lui et/ou transférer chez un autre prestataire que l’ACMOSS.

Pour ce faire, l’ACMOSS tient à la disposition du BENEFICIAIRE ou des tiers compétents désignés la procédure d’accès, ainsi que la documentation associée, qui lui permettent d’assurer la récupération et le transfert de ses Données de santé vers sa propre infrastructure ou celle d’un autre prestataire.

En cas de terminaison de la Convention principale, pour quelque raison que ce soit, y compris à la l’initiative de l’ACMOSS, l’ACMOSS maintiendra uniquement les prestations de stockage de données et l’accès à la Plateforme pendant un (1) mois à compter de la date de la fin de la Convention principale lui permettant uniquement de récupérer l’ensemble de ses Données de Santé.

À l’issue de ce délai d’un (1) mois, le BENEFICIAIRE transmettra à l’ACMOSS un procès-verbal signé de « ***Restitution intégrale des données de santé*** ». À compter de la réception de ce procès-verbal, l’ACMOSS mettra fin à l’accès nécessaire à la récupération des Données et effacera toutes les Données du BENEFICIAIRE et n’en conservera aucune trace.

Si à l’issue de ce délai d’un (1) mois, le BENEFICIAIRE n’a pas :

* adressé de procès-verbal signé de « ***Restitution intégrale des données de santé*** » ou de demande de suppression du compte auprès du support de l’ACMOSS,
* émis de procès-verbal signé de « Récupération des données terminée »,

le cas échéant après mise en demeure par l’ACMOSS, par lettre recommandée avec avis de réception au BENEFICIAIRE restée infructueuse pendant les quinze (15) jours ouvrés suivants sa réception,

L’ACMOSS pourra facturer l’immobilisation des espaces de stockages sur lesquels les Données de Santé sont encore présentes pendant 13 (treize) mois maximum.

Toutes les données du BENEFICIAIRE sont effacées définitivement au plus tard 3 Mois (90 jours) après la fin de la Réversibilité. Il s’agit du délai de conservation de la sauvegarde.

Par ailleurs, l’ACMOSS peut proposer une Prestation d’assistance du BENEFICIAIRE à la Réversibilité soumise à la passation d’un Bon de Commande.

ARTICLE 8. Suppression des données

Le BENEFICIAIRE peut supprimer son compte BENEFICIAIRE par ses propres moyens au travers les interfaces mise à sa disposition ou le cas échéant en contactant le support BENEFICIAIRE pour demander la suppression du compte BENEFICIAIRE du BENEFICIAIRE à tout moment

A la fin des prestations, l’ACMOSS s’engage à supprimer les données à caractère personnel et notamment de santé et sans en garder de copie.

Le BENEFICIAIRE autorise l’ACMOSS à procéder à la destruction des données du BENEFICIAIRE conformément à la phase de Réversibilité.

L’ACMOSS délivre une attestation de bon effacement des données à la demande du BENEFICIAIRE.

 ARTICLE 9. Mise en œuvre de mesures de sécurité

Le BENEFICIAIRE s'engage à mettre en œuvre des mesures de sécurité conformes aux bonnes pratiques en vigueur et aux référentiels applicables en matière de protection des données (y compris les données de santé à caractère personnel) et les textes réglementaires s'y rattachant et ce, sans que l’HÉBERGEUR n’ait d’obligation de contrôle sur ce point.

Ces mesures comprennent naturellement toutes les dispositions organisationnelles propres au secteur d'activité du BÉNÉFICIAIRE, celui-ci étant pleinement responsable de leur mise en œuvre dans le cadre de l'utilisation des services fournis par l'HÉBERGEUR.

Ces mesures visent à garantir la confidentialité, l'intégrité et la disponibilité des données de santé traitées dans le cadre des services fournis par l'HÉBERGEUR ».

**Certification et homologation des systèmes d’information (SI) :**
Les systèmes d’information de l’ACMOSS font l’objet d’une homologation de sécurité conforme aux exigences réglementaires applicables. Cette homologation est obligatoire en vertu de textes réglementaires tels que notamment **le Référentiel Général de Sécurité (RGS) et la Politique de Sécurité des Systèmes d’Information de l’État (PSSIE)**.

ARTICLE 10. Contacts

Le BENEFICIAIRE communique à l’ACMOSS lors de la conclusion du Contrat les coordonnées du référent contractuel à contacter notamment pour le traitement des incidents ayant un impact sur les données de santé. Ce référent doit être en mesure de désigner à l’ACMOSS un professionnel de santé lorsque cela est nécessaire.

Par convention le professionnel de santé référent désigné sera le référent santé de l’ACMOSS.

NOM : **RICHARD**

PRÉNOM: **Christophe**

FONCTION: **REFRENT SANTE de l’ACMOSS**

ADRESSE EMAIL : **referent-sante-acmoss@interieur.gouv.fr**

A ce titre le référent Santé de l’ACMOSS :

* Est garant de la confidentialité des données de santé traitées par l’HÉBERGEUR à toutes les étapes de leur traitement, il assiste les PARTIES dans toute démarche ayant un lien direct ou indirect avec l’exercice de ses missions afin de garantir le secret médical (dans le cas où les données de santé doivent être accédées).
* Veille notamment :
* Au respect des conditions d’accès aux données de santé ainsi qu’aux règles d’autorisations d’accès définies dans le contrat d’hébergement ;
* Au respect des droits des personnes, en concertation avec le responsable de traitement (et/ou son représentant) et le délégué à la protection des données ;
* A la garantie de l’indépendance des professionnels de santé conclue dans les conventions entre l’HÉBERGEUR et ses BENEFICIAIRES.
* Sera le seul autorisé à intervenir sur les données de santé hébergées au sein de l’ACMOSS Il interviendra conformément à l’article R.4127-95 du code de la santé publique.
* Il agira conjointement et en bonne confraternité avec le contact professionnel de santé du BENEFICIAIRE s’il est identifié

Les coordonnées du « Référent Médical » - professionnel de santé du BENEFICIAIRE sont les suivantes :

NOM : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\*)

PRÉNOM: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\*)

FONCTION: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\*)

ADRESSE EMAIL : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\*)

NUMERO DE TELEPHONE : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\*A renseigner par le BENEFICIAIRE)

Le BENEFICIAIRE notifie sans délai l’ACMOSS de la modification des coordonnées de son contact professionnel de santé.

Cette liste de contact pourra être transmise à l’autorité compétente qui en fait la demande, notamment dans le cas d’une suppression ou d’un retrait de la Certification HDS.

ARTICLE 11. Notification du BENEFICIAIRE

L’ACMOSS s'engage à informer ou à consulter ses BENEFICIAIRES en cas de transmission de données personnelles le concernant dans le cadre d'une réquisition, saisie ou décision judiciaire, sauf à ce que la notification soit interdite par ladite saisie.

Les modalités d’information ou de notification du BENEFICIAIRE quand la communication des données doit nécessairement être autorisée par la réquisition, saisie ou décision judiciaire concernée. Un résumé des opérations réalisées pourra être réalisé par échange de courriels, par courrier ou par lettre recommandée avec accusé de réception.

La procédure de notification du BENEFICIAIRE en cas de transmission de données personnelles dans ce contexte pourra être communiquée au BENEFICIAIRE sur demande.

ARTICLE 12. Audits sur les systèmes du BENEFICIAIRE

**Consultation de documents de conformité au BENEFICIAIRE**

L’ACMOSS met en place des mesures techniques et organisationnelles afin de répondre aux objectifs de sécurité et de protection des données personnelles, telles que définies dans ses politiques de sécurité.

L’ACMOSS met à la disposition du BENEFICIAIRE la documentation nécessaire permettant de démontrer le respect de toutes ses obligations Cette documentation pourra être portée à la connaissance du BENEFICIAIRE sur demande, après la signature d’un accord de confidentialité et sous réserve que le BENEFICIAIRE dispose des habilitations de sécurité correspondant à la typologie des documents concernés.

Cette mise à disposition prendra la forme d’une consultation des rapports d’audit, de certification, de qualification ou d’agrément accès uniquement dans les locaux de l’ACMOSS.

Les dates de consultation de cette documentation sont communicables au BENEFICIAIRE sur simple demande.

Cette consultation s’effectuera uniquement sur rendez-vous auprès du référent médical de l’ACMOSS

ARTICLE 13. Utilisation des données de santé

L’ACMOSS s’engage à ne pas traiter les données de santé hébergées à d’autres fins que l’exécution de l'activité d'hébergement de données de santé.

L’ACMOSS ne pourra notamment pas utiliser les données à des fins marketing, publicitaires, commerciales ou statistiques.

ARTICLE 14. Modalités d’accès aux données de santé

Seuls le BENEFICIAIRE et le référent santé ont accès aux données de santé hébergées sur le ou les comptes BENEFICIAIRE. L’ACMOSS s’interdit d’accéder aux données de santé du BENEFICIAIRE.

Le référent santé de l’ACMOSS est autorisé à accéder aux données de santé conformément aux termes de *l’« ARTICLE 9. Contacts »* de la présente convention.

Mises à part les mesures de sécurité mises en œuvre par l’ACMOSS pour sécuriser l’accès aux comptes prévues dans la Convention principale, le BENEFICIAIRE est seul responsable de l’accès à ses données de santé.

L’accès aux Prestations est assuré par les clés d’accès au service, soit l’ensemble des identifiants (login, mot de passe, API, etc.) permettant au BENEFICIAIRE de s’authentifier avant de pouvoir consommer et piloter des prestations. Les clés d’accès sont dédiées à̀ un compte précis. Le BENEFICIAIRE s’engage à ne pas les partager.

Le BENEFICIAIRE met en œuvre les moyens de contrôle d’accès et de gestion des identités pour les utilisateurs sous sa responsabilité́ qui utilisent des interfaces de gestion des comptes et des droits d’accès hors de celles fournies par l’ACMOSS.

Article 15. Communications partagées/communes avec d’autres communautés

L’article L1110-4 du code de la santé publique pose le principe du partage d’information entre des professionnels de santé et d’autres professionnels. Des professionnels peuvent échanger des informations uniquement dans le cas où ils participent tous à la prise en charge d’une même personne. Une condition supplémentaire précise que les informations échangées doivent être nécessaires à la coordination ou à la continuité des soins du patient, à la prévention ou à son suivi médico-social et social.

Les communautés RRF qui seraient amenées à échanger des informations sur l’état de santé du patient s’engagent à respecter les dispositions de l’article L11110-4 du code de la santé publique.

ARTICLE 16. Collaboration pour l’exercice des droits des personnes concernées

Dans le cadre de son obligation de collaboration pour l’exercice des droits des personnes concernées par des traitements de données personnelles, l’ACMOSS aidera le BENEFICIAIRE à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées : droit d’accès, droit de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données personnelles, droit de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage). Si les personnes concernées exercent auprès de l’ACMOSS des demandes d’exercice de leurs droits, l’ACMOSS adressera ces demandes dans les meilleurs délais par courrier électronique au BENEFICIAIRE afin de lui permettre de répondre aux demandes dans le délai légal d’un mois. L'HÉBERGEUR s’engage à mettre à disposition du BENEFICIAIRE les procédures pour lui permettre de répondre aux demandes d’exercice des droits des personnes concernées, à la demande de ce dernier. De plus, il est précisé que le BENEFICIAIRE qu'en tant que responsable du traitement des données personnelles de santé éventuellement concernées par la présente Convention, aura dans certains cas l'obligation de réaliser une analyse d'impact préalable sur la protection des données personnelles de santé qu'il traite, démarche dans laquelle l’ACMOSS pourra éventuellement l'assister sur demande.

ARTICLE 17. Modifications et évolutions techniques

Le BENEFICIAIRE reconnaît et accepte par la présente Annexe que l’ACMOSS pourra être amené à modifier les services ou à mettre en place de nouveaux services afin d’apporter les évolutions techniques nécessaires à la réalisation de ces services ou lorsque ces évolutions ou modifications sont imposées par le cadre légal applicable à l'HÉBERGEUR.

L’introduction de nouveaux Services ou la modification ou la maintenance de services existants font l’objet d’une communication au BENEFICIAIRE *a minima* une (1) semaine avant leur mise en service.

La planification de ces nouveaux services ou la modification des services existants est réalisée en adéquation avec les exigences de services

Dans le cas où des évolutions imposées par le cadre légal applicable à l'HÉBERGEUR entraîneraient un changement de circonstances imprévisibles lors de la conclusion de la Convention principale, la Partie qui n’a pas accepté d’assumer un risque d’exécution excessivement onéreux pourra demander une réévaluation de la Convention principale à son cocontractant.

ARTICLE 18. Garanties et procédures en cas de défaillance

L'HÉBERGEUR met en place des garanties et des procédures permettant de couvrir toute défaillance éventuelle de sa part notamment par les niveaux de services auxquels il s’engage, les assurances auxquelles il a souscrit et ses certifications notamment la certification ISO 27001 et la certification HDS avec des procédures qui couvrent non limitativement les exigences de sécurité des systèmes d’information, la continuité d’activité, la gestion des vulnérabilités.

ARTICLE 19. Intégrité des échanges

Les données personnelles transitant par un réseau de communication feront l’objet d’un chiffrement avec des protocoles permettant notamment de s’assurer que ces données sont bien reçues par le système cible.

ARTICLE 20. Modalités du transfert des données

L’ACMOSS garantit que les données BENEFICIAIRE, hébergées sur son réseau, ne seront pas transmises à des tiers par l’ACMOSS.

ARTICLE 21. Mesures techniques et organisationnelles de sécurité et de protection des données

Les principales mesures de sécurité techniques et organisationnelles ainsi que les mesures complémentaires liées à la protection des données sont décrites dans la Convention principale.

L’évolution de ces mesures techniques et organisationnelles ne peut conduire à la diminution du niveau de sécurité sauf accord préalable du BENEFICIAIRE.

L’ACMOSS s’engage à mettre à disposition à la demande du BENEFICIAIRE la déclaration d’applicabilité synthétisant les mesures techniques et organisationnelles de sécurité mises en œuvre par l’ACMOSS au travers des référentiels auxquels elle se conforme. La déclaration d’applicabilité est annexée au présent document et la dernière version à jour sera accessible sur demande.

ARTICLE 22. Traçabilité

Les actions réalisées par le BENEFICIAIRE sur la plateforme font l’objet d’une journalisation. Le BENEFICIAIRE a la possibilité de demander ces journaux à l’ACMOSS par une demande au support par le biais de l'ouverture d’un ticket support. L’ACMOSS fournira au BENEFICIAIRE sur demande les logs d’accès à l’API. Il est de la responsabilité du BENEFICIAIRE de satisfaire à l’obligation de tracer les actions des utilisateurs des applications de santé auxquelles l’ACMOSS n’a pas accès.

Article 22 : Limite d’utilisation

Les terminaux prêtés par l’ACMOSS, sont en mesure d ‘assurer des échanges multimédias (Audio, Vidéo Data).

Pour autant, les terminaux et / ou les services proposés ne peuvent être considérés comme des dispositifs médicaux (DM).

Par conséquent, l’utilisation du dispositif par le BENEFICIAIRE et ses professionnels de santé dans l’exercice de leurs missions opérationnelles réelles ne peut être envisagée, ni comme un éventuel substitutif ou supplétif aux Dispositifs Médicaux de dotation habituellement utilisé. A contrario, l’usage du dispositif est envisageable dans le cadre de l’évaluation, pour tout type de situation, dès lors que l’état de santé d’une personne prise en charge ne serait en aucun cas exposé défavorablement ou ne constituerait une quelconque perte de chance.

Article 23 : Charte d’utilisation de RRF

Les communautés utilisatrices s’engagent à respecter la Charte d’utilisation du RRF.