**ANNEXE 3 - PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL**

**Table des matières**

[1. Approche générale 1](#_Toc192090098)

[2. Objet 1](#_Toc192090099)

[3. Description du Traitement faisant l’objet de la sous-traitance 2](#_Toc192090100)

[4. Rôles et responsabilités des Parties 3](#_Toc192090101)

[5. Sous-traitance Ultérieure 4](#_Toc192090102)

[a. Principes généraux 4](#_Toc192090103)

[b. Prestataire d’hébergement de Données 5](#_Toc192090104)

[6. Droits des personnes concernées 5](#_Toc192090105)

[7. Notification des incidents de sécurité et des violations de Données 6](#_Toc192090106)

[8. Aide du Partenaire dans le cadre du respect par l’AP-HP de ses obligations 6](#_Toc192090107)

[9. Sort des Données 6](#_Toc192090108)

[10. Audits et contrôles 7](#_Toc192090109)

[11. Responsabilité 7](#_Toc192090110)

[12. Sécurité 7](#_Toc192090111)

1. **Approche générale**

La présente annexe complète les dispositions en matière de protection des Données personnelles prévues au marché visé entête des présentes (ci-après, le « Marché »).

En cas de contradiction entre le présent document et toute autre disposition du Marché en lien avec la protection des Données personnelles, les termes du présent document prévaudront.

1. **Objet**

La présente annexe a pour objet de définir les conditions dans lesquelles le Partenaire, agissant en tant que sous-traitant (ci-après, le « Partenaire » ou le « Sous-traitant ») au sens du Règlement général sur la protection des Données de l’UE (2016/679) (ci-après, « RGPD »), s’engage à effectuer pour le compte de l’AP-HP (ci-après, le « Responsable de Traitement » ou « l’AP-HP ») les opérations de Traitement de Données personnelles (ci-après, les « Données » ou « Données personnelles ») définies ci-après.

Le Partenaire est informé du caractère sensible des Données traitées, garantit qu’il respecte la réglementation (RGPD et loi IFL notamment) et reconnaît que les garanties de sécurité, de confidentialité et de disponibilité apportées constituent une condition essentielle de l’engagement de l’AP-HP.

Les termes utilisés dans la présente annexe ont le sens qui leur est donné par le RGPD à l’article Définition, notamment : « Responsable de Traitement », « Sous-traitant », « Données personnelles » (ou « Données »), « Violation de Données », « Traitement » et « Personne concernée ».

1. **Description du Traitement faisant l’objet de la sous-traitance**

Le traitement concerne l’utilisation de la solution logicielle « Chatbot AIDA IA », un chatbot multilingue basé sur l’intelligence artificielle, destiné à aider les soignants à interagir avec les patients allophones dans le cadre du dépistage des maladies infectieuses.

Toutes les données collectées seront traitées conformément à la législation en vigueur sur la protection des données personnelles. Des mesures de sécurité strictes seront mises en place pour protéger ces informations, et seules les personnes autorisées auront accès à ces données dans le cadre de la recherche et de l'amélioration du chatbot.

Le Partenaire est autorisé à traiter pour le compte de l’AP-HP les Données nécessaires pour la Fourniture du Service hébergé « Chatbot AIDA IA » incluant un chabot multilingue basé sur l’IA, objet du présent marché :

* La nature des opérations réalisées sur les Données est Indirectement via le logiciel :
  + Enregistrement de la donnée
  + Modification de la donnée
* La ou les finalité(s) du Traitement sont la vérification du bon déroulement du traitement de la donnée par la solution logicielle, y compris ses logiciels d’interface et ses outils de reprise ;
* Les Données traitées sont :
  + Informations d'identification :
    - Sexe
    - Genre
    - Âge
    - Année et mois de naissance
  + Données d'entrée en France :
    - Statut d’immigration
    - Couverture assurance maladie
    - Durée de résidence en france
  + Résultats de dépistage : hépatite B, hépatite C, VIH
  + Historique de dépistage :
    - Antécédents de dépistage pour les maladies suivantes: hépatite B, hépatite C, VIH
    - Résultats des tests et suivi médical
  + Facteurs de risque :
    - Habitudes sexuelles
    - Usage de substances (drogues)
    - Antécédents de partenaires à risque (identifiés avec les maladies mentionnées)
    - Statut vaccinal pour ces maladies
  + Données socio-économiques :
    - Niveau d'éducation
    - Situation professionnelle en France
  + Littératie en santé :
    - Connaissances en santé
    - Appréhension et attitudes vis-à-vis du dépistage
  + Interaction avec le chatbot :
    - Échanges avec le chatbot, y compris les transcriptions des discussions avec les soignants
  + Coordonnées de contact :
    - Email ou numéro de téléphone (anonymisées pour garantir la confidentialité)
* Localisation des Données personnelles : France
* Durée de conservation des Données : durée d’exécution du marché et durée du recueil des données de la cohorte et transfert de la base de données finale à l’AP-HP
* Destinataires des Données côté Partenaire : personnes autorisées du Partenaire à accéder en raison de leurs fonctions
* Sous-traitant : xxxxx (Hégergeur de Données de Santé)
* Sous-traitant ultérieur : à indiquer à l’AP-HP sans délai dès identification du nouveau sous-traitant.

Pour l’exécution des prestations objet du présent marché, le responsable de traitement met à la disposition du titulaire les informations suivantes :

* Accès aux résultats de l’étude APIDE de l’AP-HP
* Accès au dépôt de l’AP-HP pour y déposer les données.

Les Coordonnées du DPO du Partenaire sont : XXXXXX

Les Coordonnées du DPO de l’AP-HP sont : protection.donnees.dsi@aphp.fr

1. **Rôles et responsabilités des Parties**

Le Partenaire s'engage à :

* Effectuer pour le compte et sur les instructions de l’AP-HP les opérations de Traitement de Données strictement nécessaires pour fournir ses services prévus au Marché. Le Partenaire garantit qu’il ne traitera pas les Données pour son propre compte ;
* Si le Partenaire considère qu’il n’est pas en mesure de satisfaire à une instruction ou si selon lui, une instruction constitue une violation, il doit en informer l’AP-HP sans délai ;
* Traiter les Données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance et ne pas les traiter à des fins incompatibles avec la finalité du Traitement ;
* Garantir la sécurité, la disponibilité, l’intégrité et la confidentialité des Données traitées et d’empêcher qu’elles ne soient déformées, endommagées, perdues ou communiquées à des tiers non autorisés, par son fait ou celui de ses éventuels Sous-traitants Ultérieurs autorisés ;
* Veiller à ce que les personnes autorisées à traiter les Données personnelles appartenant aux équipes du Partenaire :
* N’aient accès qu’aux Données dans la mesure strictement nécessaire à l’exécution des services prévus au Marché et
* S’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
* Ne pas transférer les Données hors de l’UE, par son intermédiaire ou celle de son Sous-traitant Ultérieur, étant précisé que tout accès distant aux Données depuis l’extérieur de l’UE est considéré comme un transfert ;
* Prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des Données dès la conception (Privacy by design) et de protection des Données par défaut (Privacy by default) ;
* Aider l’AP-HP à garantir le respect de ses obligations, notamment en matière de sécurité, et pour la réalisation d’analyses d’impact et, le cas échéant, pour la réalisation de consultation préalable de la CNIL ou toute autre formalité ou revue de conformité à effectuer ;
* Mettre à la disposition à première demande de l’AP-HP la documentation nécessaire pour démontrer le respect de toutes ses obligations, notamment dans le cadre des audits, y compris des inspections, par l’AP-HP, par un tiers mandaté par l’AP-HP ou par les autorités de contrôle (la CNIL en l’espèce) ;
* Informer l’AP-HP sans délai de toute demande de communication contraignante qui émanerait d’une autorité administrative ou judiciaire et ne communiquer les Données qu’après autorisation écrite de l’AP-HP ;
* Informer immédiatement par écrit l’AP-HP de toute modification le concernant et pouvant avoir un impact sur le Traitement des Données personnelles ;
* Informer sans délai l’AP-HP si les Données reçues sont inexactes ou obsolètes, et coopérer avec l’AP-HP pour les rectifier ou les effacer ;
* Solliciter en temps opportun toutes les informations nécessaires à la bonne réalisation des Services et identifier tout risque sur son périmètre de responsabilité
* Formuler sans délai tous conseils, alertes, mises en garde, préconisations et informations dans le cadre de la réalisation du Marché, notamment en vue d'améliorer la sécurité et la confidentialité des Données ou de manière à permettre à l’AP-HP de prendre les décisions qui lui incombent ;
* Coopérer étroitement avec l’AP-HP et solliciter toute réunion qui se révélerait utile ;

Le Partenaire reconnait que les Données personnelles de l’AP-HP sont et demeurent la propriété exclusive de cette dernière. Le présent document n’emporte aucune cession, transfert ou licence que ce soit à titre onéreux ou gratuit des Données appartenant à l’AP-HP.

1. **Sous-traitance Ultérieure** 
   1. Principes généraux

Les sous-traitants du Partenaire sont qualifiés de « Sous-traitants Ultérieurs » au sens de la réglementation. Aucun Sous-traitant Ultérieur autre(s) que celui (ou ceux) strictement listés ci-dessus à l’article « Description du Traitement » n’est autorisé sans l’accord express et préalable de l’AP-HP.

En cas de volonté de modification du Sous-traitant Ultérieur en cours de Marché, l’information de l’AP-HP doit indiquer notamment les activités de Traitement sous-traitées envisagées, l’identité et les coordonnées du Sous-traitant Ultérieur, la localisation des Données et la remise du contrat de sous-traitance. L’AP-HP se réserve le droit de résilier le Marché en cas de désaccord sur ce Sous-traitant Ultérieur.

En tout état de cause tout Sous-traitant Ultérieur est tenu de respecter les mêmes obligations que le Partenaire au titre de la présente annexe. Il appartient notamment au Partenaire de contrôler que le Sous-traitant Ultérieur présente en permanence les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles (audits réguliers à faire). Le Partenaire demeure pleinement responsable devant l’AP-HP de l’exécution par le Sous-traitant Ultérieur de ses obligations.

Le Partenaire n’est pas autorisé à transférer les Données personnelles hors de l’UE (lui-même ou via ses Sous-traitants Ultérieurs), étant précisé que tout accès distant aux Données depuis l’extérieur du territoire de l’UE est considéré comme un transfert. Les Sous-traitants Ultérieurs du Partenaire ne sont pas non plus autorisés à transférer à leur tour les Données à des tiers ou à d’autres sous-traitants ultérieurs sans autorisation expresse et préalable de l’AP-HP (interdiction de la sous-traitance en cascade).

Le Partenaire garantit que ni lui ni ses éventuels Sous-traitants Ultérieurs ne sont soumis à des lois et réglementations contraires aux réglementations applicables en UE, et avertira sans délai l’AP-HP en cas d’impossibilité de se conformer au RGPD et la loi IFL en raison de lois étrangères qui lui seraient applicables, à lui ou à ses Sous-traitants Ultérieurs.

* 1. **Prestataire d’hébergement de Données**

Sans préjudice des dispositions ci-dessus, le Partenaire garantit expressément que son prestataire d’hébergement des Données visé à l’article « Description du Traitement » (qualifié de Sous-traitant Ultérieur) présente les garanties cumulatives suivantes :

* Serveurs du prestataire localisés en France ou au sein de l’UE
* Prestataire d’hébergement disposant de la certification HDS
* Prestataire d’hébergement conforme au référentiel SecNumCloud publié par l’ANSSI
* Prestataire d’hébergement garantissant sans réserve son immunité contre toute réglementation ou décision extra-européenne sur le transfert des données (garantie écrite, qui pourra être communiquée à l’AP-HP à première demande)
* Prestataire d’hébergement soumis aux lois et réglementations applicables au sein de l’UE en matière de protection des données personnelles et garantissant à tout moment le respect des dispositions du RGPD
* Prestataire d’hébergement fournissant des garanties de réversibilité des services permettant l’AP-HP de récupérer ou faire récupérer l’ensemble des Données sans atteinte à la continuité de son activité
* Conformité des services d’hébergement avec les règles de GAIA-X, notamment en termes d’interopérabilité et de portabilité.

A défaut pour le Partenaire de pouvoir s’engager sur les principes ci-dessus au jour de la signature des présentes, le Partenaire s’engage (à défaut, le contrat pourra être résilié aux tors du titulaire et sans frais ni indemnité à première demande de l’AP-HP) :

* A migrer les services d’hébergement **dans un délai de** **3 mois maximum** vers une offre présentant l’intégralité des garanties exigées ci-dessus ;
* A mettre en place sans délai avec son Sous-traitant Ultérieur les garanties appropriées exigées par l’article 46 du RGPD (par exemple, intégrer dans son contrat conclu avec son prestataire d’hébergement des clauses contractuelles types en cas de transfert publiées par la Commission européenne en juin 2021, accompagnée des mesures supplémentaires permettant de garantir un niveau de protection équivalent à celui garanti au sein de l’UE). Le Partenaire garantit à ce titre que la législation du pays tiers à laquelle son Sous-traitant Ultérieur est soumis n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité, ni ne risque de compromettre le niveau de protection adéquat que les clauses contractuelles types et les mesures supplémentaires sont précisément censées garantir ;
* A avertir sans délai l’AP-HP en cas de demande d’accès ou de risque d’accès par des autorités publiques étrangères aux Données hébergées, prendre toutes les actions légales et recours pour les contester et remettre à l’AP-HP toute documentation en ce sens.

1. **Droits des personnes concernées**

Les Personnes concernées doivent être informées par les opérations de Traitement. Le Partenaire s’engage le cas échéant à transmettre à l’AP-HP préalablement tous les éléments nécessaires à cette information à première demande de l’AP-HP.

Le Partenaire doit aider l’AP-HP à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées et fournir tous les moyens nécessaires à la gestion de ces demandes : droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, etc.

Le Partenaire informera l’AP-HP sans délai et au plus tard dans les 24 heures suivant la réception s’il reçoit une demande d’exercice des droits par courrier électronique - ***protection.donnees.dsi@aphp.fr*** Le Partenaire ne répondra à aucune demande directement sauf pour confirmer que la demande concerne bien l’AP-HP si tel est bien le cas. Le Partenaire garantit qu’il aidera l’AP-HP à traiter ces demandes conformément à la règlementation et dans le respect des délais impartis.

En cas de litige avec une Personne concernée ou tout autre tiers, le Partenaire doit coopérer pleinement avec l’AP-HP et assumer ses responsabilités si le litige a pour origine un manquement de sa part.

1. **Notification des incidents de sécurité et des violations de Données**

Le Partenaire notifie à l’AP-HP toute violation de Données sans délai et au maximum dans les 24 heures après en avoir pris connaissance. Cette notification doit être faite auprès de [aphp-signalement-securite@aphp.fr](mailto:aphp-signalement-securite@aphp.fr), et être accompagnée de toute documentation utile afin de permettre à l’AP-HP, si nécessaire, de notifier cette violation à la CNIL et/ou aux Personnes concernées.

La procédure de notification d'incident de sécurité doit inclure :

* Une description de la violation de sécurité, la nature et les circonstances de cette violation ;
* Le type de Données ayant fait l'objet de la violation de sécurité et l'identité de chaque personne affectée ou le nombre approximatif de personnes et de Données personnelles concernées ;
* Le nom et les coordonnées du Délégué à la protection des Données du Partenaire et/ou de tout autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* Une description des conséquences probables de la violation de sécurité ;
* Une description des mesures pour remédier à la violation de sécurité, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs éventuels ;
* Toute autre information que l’AP-HP peut raisonnablement demander concernant la violation de sécurité.

Le Partenaire enquête immédiatement sur la violation et identifie, prévient et fait ses meilleurs efforts pour atténuer les effets de toute violation de sécurité conformément à ses obligations résultant du présent article et, sous réserve de l'accord ou des instructions préalables de l’AP-HP, effectue toute action propre à remédier à la violation.

Le Partenaire ne publiera aucune communication externe, communiqué de presse ou rapport concernant toute violation de sécurité concernant les Données personnelles de l’AP-HP sans son autorisation écrite préalable. L’AP-HP décidera de notifier seul ou via le Partenaire le cas échéant la violation de sécurité auprès de l’autorité de contrôle concernée et/ou des personnes concernées.

1. **Aide du Partenaire dans le cadre du respect par l’AP-HP de ses obligations**

Le Partenaire aide l’AP-HP pour la réalisation d’analyses d’impact relative à la protection des données en fournissant tous les éléments relatifs à la sécurité et aux conditions d’utilisation des Données traités pour le compte de l’AP-HP.

Le cas échéant, le Partenaire aide l’AP-HP pour la réalisation de la consultation préalable de l’autorité de contrôle en fournissant à l’AP-HP tous les éléments relatifs à la sécurité et aux conditions d’utilisation des Données traités pour le compte de l’AP-HP.

1. **Sort des Données**

Au terme du Marché, le Partenaire garantit qu’il renverra toutes les Données à l’AP-HP à première demande dans un format lisible et agréé par cette dernière.

Le renvoi doit s’accompagner de la destruction immédiate de toutes les copies existantes dans les systèmes d’information du Partenaire. Une fois détruites, le Partenaire doit justifier par écrit auprès de l’AP-HP de la destruction. Le Partenaire n’est pas autorisé à anonymiser les Données sans avoir fait valider au préalable sa procédure d’anonymisation par l’AP-HP.

Le Partenaire **mettra à la disposition de l’AP-HP à première demande toute la documentation nécessaire pour démontrer le respect de ses obligations.**

1. **Audits et contrôles**

Sous réserve d’un préavis de dix (10) jours ouvrés, l’AP-HP se réserve le droit de procéder ou faire procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Partenaire de ses obligations au titre du Marché, notamment par le biais d’un audit ou d’une inspection de contrôle.

Le Partenaire s’engage à répondre aux demandes d’audit et de contrôle de l’AP-HP et effectuées par l’AP-HP elle-même ou par un tiers de confiance qu’elle aura sélectionné.

Les audits doivent permettre une analyse du respect des dispositions relatives à la protection des Données, notamment : par la vérification de l’ensemble des mesures de sécurité mises en œuvre par le Partenaire, par la vérification des journaux de localisation des Données, de copie et de suppression des Données, par l’analyse des mesures mises en place pour supprimer les Données, pour prévenir toutes transmissions illégales de Données à des juridictions non adéquates ou pour empêcher le transfert de Données vers un pays non autorisé. L’audit doit enfin pouvoir permettre de s’assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

À ce titre, le Partenaire met à la disposition du Responsable de Traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

Le Partenaire s'engage à collaborer de bonne foi avec tout auditeur ainsi désigné. Il facilitera l'accès des auditeurs à tout document ou information ou autre élément utile au bon déroulement de la mission d'audit et lui facilitera sa mission en particulier en répondant à toute question et en lui accordant l'accès à tous les outils et moyens nécessaires à l'audit. Si les conclusions de l'audit démontrent un manquement du Partenaire à ses obligations contractuelles (i) les mesures correctives seront étudiées en comité de pilotage qui statuera sur la suite qu'il convient d'y donner et des éventuelles mesures correctives à mettre en œuvre, sans surcoût, (ii) les frais d’audit seront mis à la charge du Partenaire.

En cas de contrôle de l’AP-HP par toute autre autorité réglementaire (notamment, CNIL), le Partenaire s'engage à faciliter l'accès aux environnements d'exploitation à ces autorités et à coopérer pleinement avec l’AP-HP. Le Partenaire s'engage à ne communiquer directement aux dites autorités aucune information sans avoir obtenu l'accord préalable et écrit de l’AP-HP, sauf en cas de disposition légale ou réglementaire impérative. Pour les besoins du contrôle, le Partenaire s'engage à communiquer sans délai à l’AP-HP tous les éléments qui lui seront réclamés à cette occasion sur le support requis par lesdites autorités.

1. **Responsabilité**

La responsabilité du Partenaire sera limitée aux dommages directs résultant d’un manquement de Partenaire ou de ses Sous-traitants Ultérieurs. Ne sauraient être qualifiés de dommages indirects les dommages liés à la sécurité, la confidentialité et à l’intégrité des Données de l’AP-HP.

Aucune limite de responsabilité ne s’appliquera en cas d’atteinte à la confidentialité, à la sécurité et à l’intégrité des Données de l’AP-HP, en cas de dol ou de manquement aux obligations essentielles du Partenaire.

1. **Sécurité**

*Mesures générales :*

Le Partenaire s'engage à prendre les mesures techniques et organisationnelles optimales afin de garantir **un niveau de sécurité adapté au risque et au caractère sensible des Données** notamment :

* La pseudonymisation et le chiffrement des Données ;
* Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité des systèmes et des services de Traitement ;
* Des moyens permettant de rétablir la disponibilité des Données et l'accès à celles-ci dans des délais appropriés en cas d'incident ;
* Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement ;
* La sécurité physique et logique (informatique et réseaux de communication) ;
* La mise en place de mesures pour protéger les Données contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé, dont le hacking ou la tentative de hacking des Données ;
* Des mécanismes de restriction et de contrôle d’accès des Données, permettant d’affecter aux individus, les droits d’accès aux Données strictement nécessaires à leur mission
* La conservation d’une documentation appropriée sur les activités de Traitements
* Obtenir les certifications nécessaires (notamment en termes d’hébergement de Données de santé si la réglementation le lui impose)
* Adopter des Clauses d’entreprises contraignantes (BCR) avec ses filiales le cas échéant.

Le Partenaire devra évaluer les risques liés au Traitement ainsi que pour les droits et libertés de la personne concernée (y compris le cas échéant en cas de transfert de Données hors UE) et mettre en œuvre les mesures nécessaires pour les atténuer. Les mesures complémentaires de sécurité précisément mises en place par le Partenaire figurent en Annexe 1 du présent document.

Le Partenaire s’engage en outre à :

* Ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les informations et documents communiqués par l’AP-HP;
* Prendre toutes les mesures pour que lesdites Données ne puissent être accessibles à d’autres personnes que les personnels attachés à leur Traitement pour les besoins de leurs missions. Ces derniers seront sensibilisés au caractère stratégique des informations et documents confiés et liés au Partenaire par un engagement de confidentialité ;
* Ne pas procéder à des copies, utilisations ou diffusion de partie ou totalité d’un fichier et/ou d’une Donnée, détenus par l’AP-HP à l’exception des copies, utilisations ou diffusion strictement nécessaires à l’exécution du Marché, auquel cas l’accord préalable et explicite de l’AP-HP est nécessaire ;
* Ne pas sortir des locaux de l’AP-HP des configurations, des supports numériques ou d’autres, d’éléments ou sous-ensembles d’une configuration, d’un matériel, ou d’une documentation, détenus par l’AP-HP sans l’autorisation préalable et écrite de celle-ci ;
* Informer l’AP-HP de toute réception par lui d’une mise en demeure, réquisition ou requête judiciaire, de toute enquête ou toute autre notification relative à la réalisation des services ;
* Assurer le chiffrement des informations présentes sur ses équipements utilisés ou transportés hors de ses locaux, comportant des informations nominatives, avec un logiciel de chiffrement éprouvé et ayant fait l’objet d’une certification CSPN par l’ANSSI (http://www.ssi.gouv.fr/fr/certification-qualification/cspn/).

Le Partenaire est seul responsable vis-à-vis de l’AP-HP de la perte de documents ou Données remis sous quelque forme que ce soit, ou de la divulgation volontaire ou involontaire d’informations communiquées.

Le Partenaire s’engage à respecter les dispositions juridiques en vigueur en matière d’accès aux données sensibles d’un moyen d’authentification forte validé par l’ASIP Santé (Cf. : PGSSI-S : Politique générale de sécurité des systèmes d’information de santé - Référentiel d’authentification des acteurs de santé).

En particulier, le Partenaire devra porter un soin particulier à l’accès à ces Données nominatives de santé lors d’opérations de télémaintenance. Le Partenaire garantit que les Données de santé ne seront pas transférées en dehors du système d’information de l’AP-HP.

*Mesures spécifiques :*

Les mesures décrites ci-après s’appliquent sans préjudice de celles précisées le cas échéant au Marché.

***Accès physiques :***

Le cas échéant, les locaux où le Partenaire est hébergé ainsi que les moyens d’accès physiques lui sont communiqués par l’AP-HP. Le Partenaire s’engage à suivre les règles suivantes :

* Ne pas essayer de s’introduire dans des salles non autorisées ou avec d’autres moyens que ceux mis à sa disposition
* Ne pas permettre l’accès aux personnes non signalées dans les locaux de l’AP-HP
* Respecter les systèmes de sécurité physique mis en place à l’AP-HP, en particulier fermer systématiquement à clé, les portes derrière lui, même en cas d’absence de courte durée
* Assurer la protection physique du matériel mis à sa disposition par l’AP-HP
* Restituer tous les objets permettant l’accès physique aux infrastructures et prêtés par l’AP-HP durant la prestation du Partenaire (cartes, clés, etc.) à la fin de l’intervention
* Ne pas dévoiler ou laisser à la disposition de tiers les moyens d’accès mis à disposition, même ponctuellement.
* Ne réaliser aucune copie ou duplicata de ces moyens d’accès
* Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité
* Recueillir l’accord préalable écrit du responsable du site concerné pour pouvoir être accompagné d’un tiers ou d’un Partenaire dans les locaux de l’AP-HP.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le Partenaire s’engage à transmettre au préalable à l’AP-HP un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

De même, toujours afin d’assurer la sécurité des biens et des personnes, l’AP-HP limite l’accès à certaines zones sensibles au moyen d’un système de contrôle par badge donnant lieu à un Traitement de Données.

Lorsque le Partenaire intervient sur site, l’AP-HP se réserve le droit d’installer l’antivirus institutionnel sur les machines utilisées par le Partenaire dans le cadre de sa prestation afin d’effectuer le scan de chaque poste et des supports d’information.

***Connexion du matériel du Partenaire sur les réseaux de l’AP-HP :***

Dans le cas où le Partenaire aurait besoin, pour l’exécution du Marché, de connecter des matériels informatiques lui appartenant sur le réseau de l’AP-HP, le Partenaire s’engage à :

* Recueillir préalablement l’accord explicite de l’AP-HP
* Respecter la Charte d’Utilisation du Système d’Information annexe n°16 du règlement intérieur
* Respecter les différents Politiques Techniques de Sécurité
* Garantir la présence d’un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24h les dernières signatures antivirales
* Utiliser un système d’exploitation dans une version maintenue et à jour des correctifs de sécurité et à même de récupérer et d’installer au moins 1 fois par semaine les derniers correctifs de sécurité
* Respecter les contraintes d’adressage MAC/IP
* Garantir que cette connexion n’a en aucune manière un impact sur les performances, la disponibilité, l’intégrité et la confidentialité du Système d’Information de l’AP-HP
* Garantir que son matériel ne présente aucun risque de compromission ou d’infection par un code informatique malfaisant, du réseau informatique de l’AP-HP et assumer ses responsabilités si tel est le cas
* Se connecter au réseau de l’AP-HP par les prises habituelles (Switch, prises RJ45, etc.). Les connexions à l’aide de modem sont interdites.

***Accès logiques :***

Le Partenaire s’engage à respecter les règles suivantes pour tous les accès logiques au système d’Information de l’AP-HP :

* Attribution par la direction du système d’information d’un compte utilisateur Active Directory, actif pour le temps exclusif de la prestation et / ou de la connexion
* Dans les cas exigés par la réglementation, attribution éventuelle de moyens d’authentification forte de type carte à puce, de façon nominative et pour le temps exclusif de la prestation
* Attribution d’un compte individuel et nominatif pour tout accès logique à un système comportant des Données de santé
* À ne pas contourner la mise en œuvre et l’action de l'ensemble des moyens techniques de l’AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d’information.

Le Partenaire s’engage à garantir la bonne utilisation des moyens d’identification et d’authentification qui lui ont été fournis, et en particulier :

* Garantir que ces codes d’accès ne sont accessibles qu’aux personnels autorisés
* S’assurer de la mise à jour régulière des personnels autorisés du Partenaire ou de ses Sous-traitants Ultérieurs, notamment suite à des départs éventuels de préposés. Les accès adéquats devront être révoqués en cas de cessation du besoin et / ou de départ du personnel concerné en le signalant à l’AP-HP
* Traiter ces informations de connexion comme des informations confidentielles
* Assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection péri métrique, protection physique, etc.).

Le Partenaire s’engage à :

* Faire respecter la protection, la non-divulgation et le non-partage du mot de passe des intervenants qui doivent en assurer une utilisation strictement personnelle. Le mot de passe est inaccessible et doit être suffisamment robuste ;
* Ne pas user de leur droit pour accéder à des applications, à des Données ou à un compte informatique autres que ceux qui leur auront été attribués dans le cadre de leurs missions ou pour lesquels ils ont reçu l'autorisation d'accès ;
* Ne pas user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur ;
* Ne pas altérer ou détruire des traces ou preuves relatives à des actions ou des événements sur les systèmes d’information de l’AP-HP, le concernant ou non ;
* Ne pas entraver le fonctionnement des équipements opérationnels et des équipements de sécurité, et dans tous les cas ne pas porter atteinte à la production informatique de l’AP-HP, à son SI, à ses Données et à son réseau

Le Partenaire doit avertir sans délai l’AP-HP de tous les dysfonctionnements constatés et/ou de toutes anomalies générées de son fait ou ne le concernant pas et relevant de la sécurité, qu’il aurait pu observer lors de l’exécution du Marché. À cet égard, la procédure d’alerte consiste à prévenir par tout moyen et dans les plus brefs délais l’AP-HP, qui s’attachera à isoler le dysfonctionnement.

***Protection contre les logiciels malveillants :***

Toutes les solutions du Partenaire, qu’elles soient logiques ou physiques, doivent s’intégrer dans la stratégie antivirale de l’AP-HP.

À ce titre, tous les supports d’informations devront avoir été analysés, en présence d’un agent de l’AP-HP, par un antivirus à jour, chaque fois qu’ils doivent être utilisés sur les matériels de l’AP-HP. Le Partenaire s’engage à procéder de même pour l’utilisation de tels supports sur son propre matériel.

***Télémaintenance :***

Dans le cas où le Partenaire réalise une prestation de maintenance sur des ressources du Partenaire installées sur le réseau de l’AP-HP, le Partenaire s’engage à respecter les règles suivantes :

* Les accès au système d’information de l’AP-HP depuis l’extérieur devront passer par les équipements de sécurité validés par l’AP-HP : aucun accès par modem n’est autorisé
* Aucun accès en télémaintenance ne doit être ouvert en permanence
* Tout accès en télémaintenance sur un équipement en production doit passer par une ouverture manuelle de l'accès, charge à l’AP-HP de déterminer le workflow optimal de gestion des demandes d’accès
* L’ouverture d’un accès en télémaintenance doit avoir une durée limitée à la durée de l’intervention
* Les actions des personnels du Partenaire qui accèdent au système d’information en télémaintenance doivent être tracées au moyen de l’attribution d’un compte nominatif.

En cas de télémaintenance permettant l'accès à distance aux ressources de l’AP-HP, le Partenaire devra mettre en œuvre tous les moyens pour :

* Obtenir l'accord préalable de l’AP-HP avant chaque opération de télémaintenance dont il prendrait l'initiative. En particulier les accès à la production sont strictement interdits, sauf accord écrit de la part de la DSI. Il en va de même pour les environnements d’intégration
* Prendre toutes dispositions afin de permettre à l’AP-HP d'identifier la provenance de chaque intervention extérieure
* Transmettre systématiquement au chef de projet ou responsable du système un rapport de télémaintenance retraçant les opérations menées, les Données accédées, les modifications réalisées sur l’environnement de production et leurs impacts éventuels, et ce quels que soient les composants modifiés (système, applications, middlewares, réseaux)
* S’assurer de l’intégrité de son poste, de la mise à jour de celui-ci par rapport aux derniers patches sécurité et protection contre les codes malveillants (antivirus, antimalware …
* Ne pas se connecter à des sources concurrentes potentiellement compromettantes telles qu’Internet, autres réseaux d’accès distant, etc.
* Mettre en application l’ensemble des pratiques permettant d’assurer la sécurité de l’accès distant et des outils associés, et se plier aux contraintes techniques imposées par la DSI, notamment sur les moyens techniques de chiffrement des communications à utiliser pour éviter la transmission des Données en clair.

L’utilisation des outils de prise de main à distance par le Partenaire doit s’entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des Données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins. En particulier, le Partenaire s’engage à respecter les règles suivantes :

* Les mots de passe de l’utilisateur assisté ne doivent pas être communiqués au télé-assistant.
* La télémaintenance du poste de travail doit s’effectuer de manière visuelle par affichage partagé entre l’utilisateur et le télé-assistant. L’utilisateur doit être en mesure de voir les opérations effectuées par le télé-assistant.
* L’opération de télémaintenance sur le poste de travail de l’utilisateur doit respecter le consentement préalable de ce dernier. Elle ne doit être possible que suite à l’acceptation explicite de l’utilisateur (dans le cas d’une offre d’assistance) ou à l’initiative de ce dernier (demande d’assistance).
* La télémaintenance ne doit être réalisée que par des personnels dûment autorisés à le faire.

***Gestion des vulnérabilités :***

L’AP-HP procède à une recherche périodique des vulnérabilités techniques de son système d’information.

L’AP-HP met en œuvre un plan de maintenance préventive des composants technologiques sous-jacent aux prestations (Systèmes d’exploitation, base de données…) en appliquant périodiquement les correctifs de sécurité publiés par les éditeurs.

***Mise à jour de sécurité****:*

Sur ordre de l’AP-HP, et selon une procédure à définir entre les parties intégrant un délai maximum d’installation, le Partenaire s’engage à procéder à l’installation des mises à jour de sécurité des logiciels et progiciels utilisés, après avoir procédé aux tests permettant de vérifier qu’elles ne généreront pas d’interruption de l’accès, d’indisponibilité ou une dégradation des performances ou des fonctions.

Le Partenaire prend en compte la mise à jour de la liste des risques effectuée et communiquée par l’AP-HP.

Le Partenaire s’engage à mettre à jour la sécurité dans le respect des règles d’intégrité et de confidentialité.

**Annexe au présent document - Mesures complémentaires de sécurité prises par le Partenaire**

**Date et Signature du candidat**