CONTRAT D'ABONNEMENT A LA SOLUTION APICRYPT®

Document daté du 04/11/2022

APICEM SARL
Développement et exploitation des outils APICRYPT®
sous le contrôle de l'association APICEM
www.apicrypt.org

3, Route de Bergues
CS 20 007
F-59412 COUDEKERQUE Cedex 2
Tél. +33(0)3 28 63 00 65
mail : infoapicrypt@apicrypt.org

SARL au capital de 8 000 € - RCS DUNKERQUE 439 752 353

TABLE DES MATIERES

ENTRE LES SOUSSIGNES :

La Société APICEM SARL,

Société à responsabilité limitée au capital de 8.000 €, dont le siège social est situé 3 route de Bergues, Centre d'affaires CREANOR, CS 20007, 59412 Coudekerque Cedex 2, immatriculée au registre du commerce et des sociétés de Dunkerque sous le n° 439 752 353, représentée par Monsieur le Docteur Alain CARON en sa qualité de gérant.

Ci-après, désignée "le Prestataire",

D'UNE PART,

Le professionnel de santé, du secteur sanitaire, social ou médico social souhaitant s'abonner à la messagerie APICRYPT dans l'objectif d'échanger des Données à Caractère Personnel relatives à la santé dans le cadre de leurs missions

Ci-après, désignée "l'Utilisateur",

D'AUTRE PART,

Individuellement dénommée « Partie » et ensemble dénommées « Parties »,

IL A ETE PREALABLEMENT EXPOSE CE QUI SUIT :

L'Association pour la Promotion de l'Informatique et de la Communication En Médecine (ci-après, « l'APICEM ») a développé un service de messagerie électronique dénommé messagerie sécurisée en santé APICRYPT® (ci-après dénommé Solution APICRYPT®). L'APICEM a cédée l'exclusivité de l'exploitation de la solution de messagerie sécurisée en santé au Prestataire qui en est l'opérateur.

La Solution APICRYPT® a été développée avec pour objectif d'améliorer la coordination des parcours de soins entre professionnels de différentes disciplines en fournissant aux utilisateurs une messagerie électronique professionnelle universelle et évolutive conçue pour être standard, et donc, compatible avec le plus grand nombre de systèmes, dans le respect des exigences légales applicables.

Ce service constitue un espace de confiance visant à faciliter les échanges interprofessionnels des utilisateurs recherchant un service de messagerie sécurisée d'échange de Données entre professionnels de santé et, plus largement, entre professionnels des secteurs sanitaire, social et médico-social collectant et échangeant des Données à Caractère Personnel relatives à la santé dans le cadre de leurs missions.

Ayant pris connaissance des caractéristiques de la Solution APICRYPT®, l'Utilisateur a émis le souhait de souscrire un abonnement à la Solution de messagerie sécurisée en santé du Prestataire.

C'est ainsi que les Parties se sont rapprochées afin de définir les conditions et modalités de leur accord et d'arrêter les termes du présent Contrat d'abonnement.

CECI EXPOSE, IL A ETE CONVENU CE QUI SUIT :

1 OBJET

Le présent contrat, en mode SaaS (Software as a Service), a pour objet de préciser les conditions de mise à disposition de la Solution APICRYPT® fournie par le Prestataire à l'Utilisateur dans le cadre de la souscription d'un abonnement à ladite Solution.

Le Contrat précise les droits et obligations de chaque Partie, les caractéristiques de la prestation objet de l'abonnement et inclut la mise à disposition de la licence d'utilisation des Applications APICRYPT® permettant l'utilisation de la Solution APICRYPT® par l'Utilisateur.

Les Parties s'engagent à collaborer loyalement et à échanger les informations nécessaires à la bonne exécution des présentes.

2 DOCUMENTS CONTRACTUELS

Le Contrat constitue l'intégralité des engagements existant entre les Parties. Il remplace et annule tout engagement oral ou écrit antérieur relatif à l'objet du Contrat et est formé des documents contractuels suivants (classé par ordre de priorité décroissant) :

- Le présent document ;
- Les annexes au présent document :
  - Annexe A : Définitions ;
  - Annexe B : Descriptif de la Solution APICRYPT® ;
  - Annexe C : Qualité ;
  - Annexe D : Charte de bon usage de la messagerie APICRYPT®.

En cas de contradiction entre des documents de nature différente ou de rang différent, il est expressément convenu entre les Parties que les dispositions contenues dans le document de rang supérieur prévaudront pour les obligations se trouvant en éventuel conflit d'interprétation.

3 PRISE D'EFFET, DUREE, RECONDUCTION, RESILIATION

3.1 EFFET

Le Contrat prend effet à la date d'acceptation de la commande lors de l'inscription de l'Utilisateur à la Solution APICRYPT® sur le site Internet www.apicrypt.org ou à la date de signature du Bon de Commande par l'Utilisateur.

La date d'acceptation de la commande ou la date de signature du bon de commande sont dénommées « Date anniversaire » ci-après.

3.2 DUREE

La durée de la prestation est de 12 mois, renouvelable à Date anniversaire de l'Abonnement par le règlement d'une nouvelle année d'Abonnement.

Cas particulier : Dans les cas où l'Abonnement de l'utilisateur est souscrit dans la période novembre-décembre, l'Utilisateur bénéficiera d'un report de sa Date anniversaire d'abonnement au 1er janvier de l'année N+1. Le surcout de cet allongement de durée d'Abonnement est pris en charge par le Prestataire. Ce dispositif est prévu afin que les utilisateurs puissent avoir le temps de recevoir et d'installer les clefs de chiffrements avant le début de l'année N+1 et ne soient pas privés de leurs flux de messagerie au 1er janvier de l'année N+1.

3.3 RECONDUCTION

Trois (3) mois avant l'expiration du Contrat, le Prestataire avisera l'Utilisateur, par tout moyen écrit, de la prochaine reconduction tacite du Contrat. Au terme d'un délai de quatre-vingts (80) jours à compter de l'envoi de cet avis, sauf dénonciation par une Partie par lettre recommandée avec avis de réception, le Contrat se renouvellera par tacite reconduction pour une période d'un (1) an.

3.4 RESILIATION

3.4.1 A L'ECHEANCE

Chacune des parties peut résilier, sans indemnité de part et d'autre, le présent Contrat pour la première fois à l'issue de la période de 12 mois, puis ultérieurement à chaque renouvellement annuel, par lettre simple.

3.4.2 PAR LE PRESTATAIRE

Le Prestataire se réserve la possibilité de résilier unilatéralement et de plein droit le Contrat, et ce, sans préjudice de tous dommages et intérêts dans les cas suivants :

- Ouverture d'une procédure de redressement judiciaire ou de liquidation judiciaire de l'Utilisateur, et sous réserve des dispositions des articles L622-13 et L641-10 du Code de Commerce ;
- Cessation totale ou partielle d'activité de l'Utilisateur ;
- Manquement par l'Utilisateur à tout ou partie de ses obligations légales, réglementaires ou contractuelles.

3.4.3 PAR L'UTILISATEUR

L'Utilisateur pourra, après accord express et préalable du Prestataire, et la fourniture de preuve, demander la résiliation de son abonnement en cas de cessation de son activité ou de l'application d'une réglementation ou décision d'ordre professionnel et dans les cas suivants :

- Ouverture d'une procédure de redressement judiciaire ou de liquidation judiciaire du Prestataire, et sous réserve des dispositions des articles L622-13 et L641-10 du Code de Commerce ;
- Manquement par le Prestataire à tout ou partie de ses obligations légales, réglementaires ou contractuelles.

3.4.4 POUR MANQUEMENT

La résiliation pour manquement pourra intervenir dans les cas suivants :

- Dans le cas où le Prestataire ou l'Utilisateur ne respecterait pas les obligations qui leur incombent en vertu des présentes et 30 jours après l'envoi d'une lettre recommandée avec accusé de réception d'avoir à remédier à la défaillance constatée restée infructueuse, le contrat pourra être résilié ;
- Dans le cas où l'Utilisateur contreviendrait aux dispositions de la charte d'utilisation de la Solution APICRYPT.

En outre, le défaut de paiement par l'Utilisateur en l'absence de contestation sérieuse constitue un cas de résiliation si bon semble au Prestataire, sans préjudice de dommages et intérêts.

3.4.5 PERTE DE L'AGREMENT OU DE LA CERTIFICATION

En cas de perte de l'agrément ou de la certification hébergeur de donnée de santé (A-HDS ou C-HDS) par le Prestataire, l'Utilisateur pourra mettre fin au présent contrat sans pénalité.

4 FIN DU CONTRAT

La fin du Contrat, quel qu'en soit le motif, entraîne pour l'Utilisateur l'obligation de cesser d'utiliser la Solution APICRYPT® et de procéder à la désinstallation des Applications et Éléments secrets APICRYPT®.

Le Prestataire procède à la destruction des Éléments secrets de l'Utilisateur. Cette action fait l'objet d'un PV de destruction, disponible sur le compte de l'Utilisateur, et accessible durant une période de 12 mois à compter de la fin de Contrat.

Les stipulations de l'article 18 – Confidentialité restent applicables pour la durée prévue au dit article, indépendamment de la fin du Contrat.

4.1 REVERSIBILITE

Le Prestataire ne stockant aucune donnée, mais assurant uniquement un transit des données par ses serveurs, la restitution des données à l'Utilisateur sera faite par l'ultime relève de ses messages puis par la suppression de la boîte aux lettres APICRYPT® par le Prestataire.

5 CONDITIONS FINANCIERES

L'offre tarifaire d'abonnement à la Solution APICRYPT® est un forfait comprenant des frais de fonctionnement annuels, correspondant à la production de clefs de chiffrement et certificats de signatures sur support physique ou dématérialisé ainsi qu'aux opérations de traitement logistique des envois dudit support, auxquels s'ajoute le montant de l'abonnement annuel.

Les tarifs de l'abonnement au service de messagerie sécurisée en santé APICRYPT® et des éventuelles prestations associées sont ceux en vigueur au moment de votre consultation et validation de commande (soit sur le site web www.apicrypt.org soit par Bon de commande).

Les tarifs sont établis en Euro et révisables annuellement.

6 MODALITES DE PAIEMENT

Nonobstant la durée d'engagement, les services sont facturés annuellement, à la date anniversaire de souscription au contrat d'abonnement, directement aux Utilisateurs de la Solution APICRYPT®.

Les factures sont payables termes à échoir, sous 30 jours à compter de la date de réception par virement bancaire SEPA ou prélèvement SEPA.

Le défaut de paiement entraîne systématiquement la coupure des services associés à la Solution APICRYPT®.

La redevance annuelle d'abonnement doit être réglée par l'Utilisateur au comptant :

- à réception de la facturation (dans le cadre de la fourniture de service sous bon de commande) ;
- à l'occasion de la commande sur le site www.apicrypt.org (abonnement initial) ;
- à réception de l'avis de paiement (renouvellement d'abonnement).

Les termes de paiement convenus ne peuvent être retardés sous quelque prétexte que ce soit, y compris en cas de litige.

Les factures ou avis de paiement sont à régler aux dates d'échéances prévues, une indemnité forfaitaire de frais de recouvrement de 40 euros en cas de retard de paiement sera appliquée conformément à la loi du 22 mars 2012 dite de simplification du droit. D'autre part, en cas de retard de règlement, il sera appliqué le taux d'intérêt légal en vigueur au montant de la facture ou avis de paiement par mois de retard.

7 OBLIGATIONS DU PRESTATAIRE

Pour la mise en œuvre de la Solution APICRYPT®, Le Prestataire assure la gestion de l'exploitation et le rôle de tiers de confiance. Il s'engage à :

- Fournir les Éléments secrets permettant les échanges entre Utilisateurs équipés d'APICRYPT® ;
- Fournir les Applications ainsi que les informations de configuration de celles-ci permettant l'utilisation de la Solution APICRYPT® par l'Utilisateur ;
- Maintenir opérationnelle la Solution APICRYPT® tout au long de la durée de validité du présent contrat ;
- Communiquer à l'Utilisateur toute modification technique impactant les envois et les réceptions de courriels ;
- Signaler à l'Utilisateur toute anomalie de fonctionnement, quelle que soit sa cause impactant les envois et réceptions de courriels ;
- Mettre à disposition de l'Utilisateur toute documentation nécessaire à la bonne mise en œuvre de la solution APICRYPT® ;
- Mettre à disposition de l'Utilisateur un espace personnel consultable sur le site www.apicrypt.org rendant accessible l'ensemble des données du compte Utilisateur principal et du ou des Alias ;
- Mettre à disposition de l'Utilisateur l'annuaire des adresses mail des Utilisateurs d'APICRYPT® ;
- Faire figurer l'Utilisateur dans l'annuaire des adresses mail des Utilisateurs d'APICRYPT®.

8 OBLIGATION DE L'UTILISATEUR

L'Utilisateur de la Solution APICRYPT® s'engage à avoir la qualité de professionnel du secteur de santé, du secteur médico-social ou social autorisé par la loi à échanger des données de santé de manière informatisée.

L'Utilisateur s'oblige par ailleurs aux engagements suivants :

- Disposer d'un équipement informatique et réseau compatible, d'une connexion au réseau Internet, et éventuellement d'un logiciel métier fonctionnant avec la messagerie sécurisée en santé APICRYPT®, en conformité avec les indications techniques (liste des logiciels compatibles tenue à la disposition de l'Utilisateur par le Prestataire) ;
- Procéder au pré-paramétrage par l'intermédiaire du logiciel d'installation fourni par le Prestataire et informer sans délai l'assistance technique du Prestataire en cas de difficulté d'installation, de même en cas d'anomalie de fonctionnement, quelle que soit sa cause ;
- Maintenir opérationnel le système de réception des courriels en provenance du Prestataire tout au long de la durée de validité du présent contrat (installation des outils APICRYPT® et des clefs de chiffrement notamment) ;
- Communiquer au Prestataire toute modification technique impactant les envois ou réceptions de courriels ;
- Signaler au Prestataire toute anomalie de fonctionnement, quelle que soit sa cause, impactant les envois ou réceptions de courriels ;
- Mettre à disposition du Prestataire tout élément nécessaire à la bonne mise en œuvre de la messagerie APICRYPT® ;
- N'utiliser en aucun cas, sous quelque forme que ce soit, la Solution APICRYPT® comme un substitut au dossier médical, sanitaire ou médico-social du patient ;
- Relever régulièrement les messages reçus en provenance d'autres utilisateurs ;
- Mettre en place une politique d'information des patients (Le Prestataire fournit des documents d'informations patients sur son site Internet www.apicrypt.org) ;
- S'assurer du respect de la charte de bon usage de la Solution APICRYPT® ;
- Dans le cas d'un établissement, s'assurer du respect de la charte de bon usage de la Solution APICRYPT® ainsi que de sa diffusion jusqu'au niveau de l'utilisateur final ;
- Mettre en place les moyens destinés à stopper tout courrier indésirable et à prendre à sa charge les développements informatiques nécessaires afin de bloquer tout courrier ne contenant pas de données médicales nominatives ou un envoi de courriels en masse ;

- Pour les Laboratoires d'Analyses Médicales, le référent du laboratoire est dans l'obligation de communiquer les noms et coordonnées des praticiens de son laboratoire ou de son groupement utilisant la Solution APICRYPT® ;
- Pour les établissements, le référent de l'établissement s'engage à mettre à disposition du Prestataire l'annuaire des Utilisateurs de la messagerie APICRYPT® au sein de l'établissement et à le maintenir à jour ;
- Régler la redevance annuelle d'abonnement.

L'Utilisateur doit respecter les instructions d'utilisations prévues dans le présent contrat, sans quoi, le Prestataire ne peut garantir la possibilité d'usage de l'adresse de courrier électronique APICRYPT®.

9 OBLIGATIONS DES PARTIES SPECIFIQUES AUX DONNEES DE SANTE A CARACTERE PERSONNEL

Au regard de sa finalité consistant à échanger des données à caractère personnel sensibles, la Solution APICRYPT® a été développée dans le respect du règlement (CE) N°2016/679 dit Règlement Général sur la Protection des Données, et des dispositions du Code de la Santé Publique, dont l'article L.1110-4 du Code de la Santé Publique qui définit les conditions d'échange de données de santé à caractère personnel entre professionnels de santé et imposent l'utilisation de moyens d'authentification forte par carte de professionnel de santé ou tout autre dispositif équivalent.

L'Utilisateur de la messagerie reconnaît avoir juridiquement la qualité de « responsable de traitement » au sens des dispositions du RGPD en tant que responsable de l'usage de la messagerie électronique qui lui est fournie par le Prestataire, détenant la responsabilité de décider de la mise en œuvre d'un service de messagerie sécurisée ainsi que du choix des moyens afférents à ce service. L'Utilisateur doit s'assurer d'un usage de la Solution APICRYPT® conforme à la réglementation et charge à lui d'effectuer les formalités administratives obligatoires.

9.1 INFORMATION DES PERSONNES CONCERNEES PAR LE TRAITEMENT

Le Prestataire n'étant par la nature jamais en relation directe avec les personnes concernées par les données hébergées, l'information des personnes concernées sur leurs droits est du ressort exclusif de l'Utilisateur, tant pour l'hébergement, que pour l'accès aux données, ou pour leur transmission éventuelle.

L'Utilisateur s'engage à respecter les dispositions de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé et notamment l'article L1110-4 modifié du Code de la santé publique. Il s'engage à informer les personnes concernées :

- sur la nature des traitements opérés sur les données recueillies ;
- qu'elles peuvent s'opposer à l'hébergement pour motif légitime ;
- qu'elles peuvent s'opposer à l'échange et au partage d'informations les concernant ;
- qu'elles peuvent exercer ces droits à tout moment.

Un modèle de note d'information concernant l'échange de données de santé par voie électronique est téléchargeable sur le site Internet www.apicrypt.org.

9.2 MISE A DISPOSITION DES DONNEES HEBERGEES – AUTHENTIFICATION FORTE - SURVEILLANCE

Par nature, les données sont collectées, saisies et mises à disposition par l'Utilisateur via ses propres applications de santé ou celles de ses fournisseurs d'application de santé, le Prestataire n'ayant aucun motif ni droit d'accès aux dites applications.

Pour les personnes concernées par les données hébergées, les conditions d'information, de recueil du consentement le cas échéant, les modalités de mise à disposition, d'accès, de rectification, de traçabilité et de transmission éventuelle sont du ressort exclusif de l'Utilisateur.

En ce qui concerne l'accès aux données de santé, l'Utilisateur s'engage à respecter les dispositions de l'article L 1110-4 du Code de la Santé Publique sur le respect de la vie privée et du secret des informations concernant le patient. Il incombe à l'Utilisateur de mettre en œuvre un moyen d'identification du patient assurant l'attribution du bon identifiant au bon patient afin d'éviter les doublons et les risques de collisions entre des dossiers de différents patients.

Conformément à l'article L.1110-4-1 du Code de la santé publique l'Utilisateur se conformera aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 et notamment concernant les moyens d'authentification et d'accès aux données de santé à caractère personnel.

Il incombe également à l'Utilisateur de mettre en œuvre une politique de surveillance, particulièrement sur les accès aux moyens fournis par les composants du Système d'Information (systèmes d'exploitation, SGBD, ...) et sur les tentatives d'accès externes.

9.3 TRAÇABILITE – MISE A DISPOSITION ET SAUVEGARDE DES TRACES

Par nature, les données sont mises à disposition de l'Utilisateur par le biais de ses propres applications de santé ou celles de ses fournisseurs d'application de santé, le Prestataire n'ayant aucun motif ni droit d'accès aux dites applications.

Pour ce qui concerne la traçabilité applicative, il incombe à l'Utilisateur de mettre en œuvre les moyens de traçabilité des accès aux données, de sauvegarde des traces, et d'accès aux traces pour les personnes concernées par les données hébergées.

Des données de traçabilité technique sont générées automatiquement par les systèmes du Prestataire (système d'exploitation, équipements réseaux et de sécurité : pare-feu par exemple) ainsi que par la mise en œuvre des composants applicatifs liés à l'utilisation de la Solution APICRYPT®. Ces traces incluent des données de connexion et de déconnexion au système de messagerie (authentification de l'utilisateur ou de la machine) ainsi que les traces des actions réalisées par les opérateurs techniques du système.

Les traces techniques sont conservées pendant un an.

À l'issue des durées de conservation susmentionnées, les données sont définitivement supprimées.

Le Client peut solliciter le Prestataire afin de disposer des traces réalisées par les opérateurs techniques en contactant les services du prestataire au travers du site web www.apicrypt.org. Le Prestataire se réserve la possibilité de fournir ces traces en fonctions des compétences de l'autorité qui les sollicite et dans la limite de la faisabilité technique.

Dans l'éventualité d'une demande de la part des autorités, et s'il est autorisé par les autorités à le faire, le Prestataire en informera le Client dans les plus brefs délais et par écrit.

9.4 SECURISATION DE LA SOLUTION APICRYPT

Il est rappelé que l'ensemble des éléments permettant à l'Utilisateur de s'identifier et d'utiliser le Système APICRYPT® est personnel et confidentiel. L'Utilisateur s'engage à conserver secret ses Éléments Secrets, et à ne pas les divulguer sous quelque forme que ce soit.

Tout usage des Éléments Secrets de l'Utilisateur est fait sous son entière responsabilité.

Pour ce faire, l'Utilisateur se devra d'employer tout moyen qu'il jugera nécessaire pour conserver ses Éléments Secrets dans des conditions de sécurité et de confidentialité adéquates.

Dans le cas où l'Utilisateur est un établissement de soins, celui-ci devra s'assurer de la mise à jour de l'annuaire des correspondants au sein de son établissement, et avertira Le Prestataire des mouvements du personnel

ayant vocation à échanger des données personnelles de santé. Tout départ du « Pool Utilisateur » signalé au Prestataire engendrera la désactivation des clés de cryptage du personnel concerné.

9.5 OBLIGATIONS SPECIFIQUES EN CAS DE MODIFICATIONS OU EVOLUTIONS TECHNIQUES/TECHNOLOGIQUES INTRODUITES PAR LE PRESTATAIRE

Le Prestataire peut être amené à modifier ou faire évoluer la Solution APICRYPT® en fonction des évolutions technologiques ou des évolutions réglementaires.

Ces modifications ou évolutions sont planifiées de manière à impacter le moins possible les activités des utilisateurs de la Solution APICRYPT®.

De manière systématique et particulièrement en cas d'impact prévisible sur les activités des utilisateurs, le Prestataire s'engage à communiquer, par tous moyens (e-mail, courrier, note d'information sur le site Internet, etc.), auprès des utilisateurs impactés afin que ceux-ci puissent prendre les dispositions qui conviennent au maintien de leurs activités. Les communications adressées aux utilisateurs mentionneront notamment la date d'intervention planifiée, la durée d'intervention prévue, la raison de l'intervention, les impacts éventuels ainsi que les modalités de contact de l'assistance utilisateur d'APICEM SARL en cas de questions ou de difficultés rencontrées par les utilisateurs.

9.6 SIGNALEMENT DES INCIDENTS RELATIFS AUX DONNEES DE SANTE

L'Utilisateur assure l'entière responsabilité des procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé collectées par lui-même.

Le Prestataire et l'Utilisateur doivent se signaler de façon réciproque tous les incidents relatifs aux données de santé qu'ils détecteraient afin de pouvoir y remédier de façon concertée. Chacune des Parties préviendra donc l'autre, dans les plus brefs délais et par écrit, des incidents relatifs aux données de santé sur le périmètre qui lui incombe. Dans ce cadre le Prestataire offrira une assistance raisonnable au Client pour toute information qui lui serait nécessaire.

9.7 CERTIFICATION HDS

Les comptes rendus d'audit de certification sont disponibles en consultation uniquement chez le Prestataire sur demande auprès du RSSI du Prestataire. Aucune copie des rapports ne pourra être remise à l'Utilisateur.

Les certificats du Prestataire sont quant à eux accessible sur le site Internet du Prestataire et annexés au présent contrat.

9.8 AUDIT ET TEST DE LA SOLUTION APICRYPT

Les Utilisateurs peuvent solliciter la conduite d'un audit de sécurité des services fournis par le Prestataire par tout professionnel accrédité à cet effet, à leur frais et dans la limite d'un (1) audit par an. Le périmètre de l'audit, ses modalités ainsi que son planning devront obligatoirement être validés au préalable par le Prestataire.

Afin de ne pas pénaliser les activités du Prestataire, L'Utilisateur devra faire part de sa demande accompagnée du planning et périmètre envisagé au minimum un (1) mois avant la date de démarrage envisagée par courrier avec accusé de réception.

Le périmètre ainsi que le planning pourront faire l'objet de réserves de la part du Prestataire étant entendu que les audits et tests sur les composants, services ou éléments mutualisés et plus généralement tout test pouvant compromettre la Disponibilité, l'Intégrité, la Confidentialité ou l'Auditabilité des systèmes d'information du Prestataire sont exclus du périmètre d'audit accordés à un Utilisateur. L'Audit devra par ailleurs être limité au seul périmètre de la certification HDS et exclura toute autre norme.

De plus, le Prestataire se réserve la possibilité de mettre un terme à un audit qui causerait un incident de sécurité ou dans l'éventualité où les outils d'audit permettraient l'exfiltration de données pouvant impacter le Prestataire ou d'autres clients du Prestataire.

Les remarques suivant la demande de l'Utilisateur sont adressées par le Prestataire par courrier recommandé avec accusé de réception au maximum 5 jours ouvrés suivant la réception de la demande de l'Utilisateur.

Le Prestataire s'engage à tenir à disposition des utilisateurs les résultats d'un audit externe et indépendant sur les composants, services ou éléments mutualisés (cf. article 9.7 « Certification HDS »).

L'Utilisateur communiquera le ou les rapports d'audit au Prestataire à l'issue de l'audit par courrier recommandé avec accusé de réception.

En cas de manquement constaté sur le périmètre du Prestataire et agréé par ce dernier, le Prestataire proposera un plan de remédiation sous un (1) mois à l'Utilisateur. L'exécution dudit plan de remédiation est de la responsabilité du Prestataire.

Le Prestataire se réserve le droit de se faire accompagner par un auditeur de son choix à l'occasion d'un audit diligenté par un Utilisateur.

La participation du Prestataire dans le cadre des audits diligentés par les Utilisateurs est par ailleurs facturée au titre de prestation complémentaire. À ce titre le Prestataire établira un devis révisable des frais envisagés selon la nature de la demande de l'Utilisateur et le plan d'audit. Les frais facturés peuvent notamment inclure : les frais liés à l'intervention des collaborateurs sollicités ou intervenants dans le cadre de l'audit, les frais éventuels liés à la fourniture d'information (impression, fourniture d'éléments de preuves, etc.), les frais éventuels liés à l'implication des sous-traitants du Prestataire, etc.

La facturation définitive est adressée à l'Utilisateur après validation par lui du plan d'action éventuelle ou transmission du rapport d'audit en l'absence de non-conformité.

Par ailleurs, toutes les données traitées dans le cadre d'un tel audit seront considérées comme confidentielles. À cet effet, l'Utilisateur garantira la mise en oeuvre de mesures de sécurité appropriées en vue de protéger les données par exemple en chiffrant ces dernières, en effaçant les données de manière sécurisée ainsi que leurs copies. L'effacement des données devra intervenir dès la fin de l'audit et au plus tard dans les 3 mois suivants la fin de l'audit. L'Utilisateur se portera par ailleurs garant du respect de la confidentialité par l'auditeur ou l'organisme qu'il sollicitera pour procéder à l'audit et s'engagera à conclure un accord de confidentialité avec le Prestataire à cet effet préalablement au déroulement de l'audit.

10 FORCE MAJEURE

Est considéré comme cas de force majeure, tout événement imprévisible, irrésistible et extérieur tel que le déclenchement de Plan de Prévention Seveso, phénomènes naturels exceptionnels, etc.

Dans ce cas si le Prestataire, ne peut trouver une solution dans des délais raisonnables afin de ne pas perturber le fonctionnement de la Solution APICRYPT®, le Prestataire assurera un transfert sécurisé des services APICRYPT®, vers sa plateforme miroir, et parallèlement assurera l'information de l'Utilisateur par un plan de communication adapté.

En aucun cas, il ne peut y avoir de perte d'information dans les données personnelles de santé. Tout au plus, cela peut contraindre l'Utilisateur à utiliser d'autres moyens de transmission des données personnelles de santé.

11 SAUVEGARDE – ARCHIVAGE – SECURITE

11.1 SAUVEGARDE

Le Prestataire a la charge de mettre en place les mesures de sauvegarde appropriées pour assurer la conservation des messages et données de l'Utilisateur ; Ainsi que la sauvegarde des clés de cryptage actives mises en place sur ses serveurs.

La sauvegarde des données des utilisateurs (données personnelles de l'utilisateur, données de configuration utilisateur) est réalisée quotidiennement. Les comptes de messagerie de l'utilisateur sont quant à eux sauvegardés toutes les heures.

Les données contenues dans les comptes de messagerie APICRYPT® de l'Utilisateur sont supprimées des serveurs du Prestataire après relève des courriers électroniques par l'Utilisateur. De fait, il appartient à l'Utilisateur de mettre en œuvre une solution de sauvegarde pour les données transitant par APICRYPT® et déjà relevée par l'Utilisateur.

Les sauvegardes des serveurs du Prestataire sont testées régulièrement conformément à la politique de sauvegarde, par le Prestataire lors de tests de restauration de données.

Les sauvegardes peuvent être totales, différentielles ou incrémentielles en fonction du système ou des données concernées et dans le respect de la réglementation.

Le Prestataire, conformément à sa politique de sauvegarde, dispose d'indicateurs concernant la réalisation des sauvegardes ou l'exécution des tests de restauration des sauvegardes.

11.2 ARCHIVAGE

Le Prestataire n'assure en aucun cas l'archivage des données, en dehors de la procédure de sauvegarde.

11.3 SECURITE

L'Utilisateur s'engage à respecter les dispositions de l'article L1110-4-1 du code de la santé publique et à mettre en œuvre les référentiels d'interopérabilité (référentiels de la PGSSI-S notamment), et de sécurité, élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24.

11.3.1 VIRUS – ATTAQUE – MALVEILLANCE

Le Prestataire et l'Utilisateur doivent chacun de leur côté mettre en œuvre toutes les mesures et tous les moyens nécessaires de nature à éviter que le système informatique ne soit contaminé par un quelconque virus, attaque ou malveillance.

11.3.2 SECURITE LOGIQUE DE L'EXPLOITATION

Les dispositions ci-dessous s'appliquent à l'ensemble des données, fichiers et programmes de l'Utilisateur.

Il est ici rappelé que la sécurisation du réseau de communication entre les sites de l'Utilisateur et du Prestataire est assurée par un fournisseur d'accès sous la responsabilité directe de l'Utilisateur, ce sans quoi le Prestataire ne peut garantir le traitement des données personnelles de santé.

Le Prestataire s'engage à avertir l'Utilisateur de toute dérive ou de tout incident qu'il pourrait constater dans l'application des règles générales de sécurité.

Le Prestataire informera l'Utilisateur de toute tentative de violation de droits d'accès qu'il serait amené à constater.

11.3.3 CONTINUITE D'EXPLOITATION

Afin de procéder à l'hébergement de données personnelles de Santé, le Prestataire dispose d'une plateforme principale, et afin d'assurer la continuité de la mise à disposition des données, elle dispose d'un PRA/PCA permettant la mise en œuvre d'une plateforme de secours.

11.3.4 SECURITE PHYSIQUE

Une Politique de Sécurité du Système d'Information (PSSI) validée par le Responsable de la Sécurité des Systèmes d'Information (RSSI) est en place, elle est connue, validée et acceptée par tous les collaborateurs du Prestataire.

Un protocole d'alarme est en vigueur au sein des locaux du Prestataire. Toutes les alarmes sur place sont relayées par des appels automatisés au RSSI, au Directeur Technique qui prennent les mesures nécessaires afin de pallier les déclenchements qu'il soit d'intrusion, d'alarme incendie et surtout de défaillance ou de problèmes techniques.

12 RESPONSABILITES

Les parties s'efforceront de régler à l'amiable les différends qui pourraient survenir à l'occasion de l'exécution du présent contrat. À défaut, les Tribunaux de Dunkerque sont seuls compétents même lorsqu'il y a pluralité de demandeurs ou de défendeurs, ou d'appels en garantie.

13 POLITIQUE DE GESTION DES DONNEES DU PRESTATAIRE

La sécurité des Données Personnelles des Utilisateurs ainsi que des Données de Santé transportées par la Solution APICRYPT® est une priorité ABSOLUE pour le Prestataire qui entend construire avec les Utilisateurs de la Solution APICRYPT une relation forte et durable basée sur la transparence et la confiance réciproque.

Aussi, le Prestataire s'engage à respecter formellement l'ensemble des dispositions réglementaires et législatives françaises et européennes relatives à la protection des données et notamment la loi n° 78-17 du 6 janvier 1978 telle que modifiée par la loi n°2004-801 du 6 août 2004 dite "Informatique et Libertés" et le Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016.

En tout état de cause :

- L'Utilisateur de la Solution APICRYPT® reste propriétaire de ses Données Personnelles, le Prestataire n'en dispose pas librement ni autrement que pour les besoins décrits dans la présente politique.
- Les Données Personnelles sont traitées de manière transparente, confidentielle et sécurisée
- Le Prestataire dispose d'une équipe dédiée à la protection des Données Personnelles composée d'un Responsable de la Sécurité des Systèmes d'Information, d'un Délégué à la Protection des Données (DPO), d'un conseil juridique ainsi que d'ingénieurs ou techniciens spécialisés.
- Les Données de Santé sont hébergées par le Prestataire qui dispose de l'agrément Hébergeur de Données de Santé (HDS) délivré par l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé)

La Politique de Gestion des Données Personnelles du Prestataire est consultable et téléchargeable sur le site www.apicrypt.org.

14 CONDITIONS D'UTILISATION

L'utilisateur s'engage à :

- Ne pas pratiquer l'envoi de messages non sollicités à un ou plusieurs destinataires. Il est rappelé à l'utilisateur que la violation de cette stipulation peut entraîner la suspension puis la résiliation de

son compte utilisateur. À cet égard, une charte de bon usage a été éditée, l'Utilisateur se doit d'en prendre connaissance. Elle figure en Annexe D ;

- Ne pas télécharger, transmettre par le système APICRYPT® ou par tout autre moyen des courriers électroniques et/ou fichiers contenant des virus ou plus généralement tout programme visant notamment à interrompre, détruire ou limiter la fonctionnalité de tout logiciel, ordinateur ou réseau de télécommunication.

En cas d'envoi de messages non-sollicités, plus communément désigné Spam, le Prestataire appliquera les modalités suivantes :

- 1er envoi de spam :
  - le Prestataire bloque le message, s'assure en coordination avec l'utilisateur que le message est un message non-désiré. Si le spam est avéré, le Prestataire procède à un rappel, par email, à l'utilisateur des conditions d'utilisation de la messagerie APICRYPT®.
- 2ème envoi de spam :
  - Le Prestataire bloque le message, s'assure en coordination avec l'utilisateur que le message est un message non-désiré. Si le spam est avéré, le Prestataire adresse un courrier recommandé à l'utilisateur et bloque éventuellement l'accès au serveur de messagerie APICRYPT® de l'Utilisateur jusqu'à règlement des frais de gestion induits. A cette occasion, l'Utilisateur se voit facturer les frais de gestions induits (voir article 14.1).
- 3ème envoi de spam :
  - Le Prestataire bloque le message, s'assure en coordination avec l'utilisateur que le message est un message non-désiré. Si le spam est avéré, le Prestataire procède au blocage immédiat et de l'accès aux serveurs de messagerie APICRYPT® de l'Utilisateur jusqu'à règlement des frais de gestion induits. A cette occasion, l'Utilisateur se voit facturer les frais de gestions induits (voir article 14.1).

Dans le cas d'un établissement, l'utilisateur référent s'engage à respecter et faire respecter par son personnel toutes mesures de sécurité et de discipline inhérentes à l'utilisation d'une messagerie sécurisée hébergée.

14.1 FRAIS DE GESTION TRAITEMENT DES SPAMS

En cas d'envoi de messages non-sollicités, plus communément désigné Spam, le Prestataire appliquera les modalités de tarifications suivantes :

- 1er envoi de spam :
  - Le Prestataire ne facture pas de frais de gestions.
- 2ème envoi de spam :
  - Le Prestataire facture des frais de gestions selon les modalités suivantes :
    - Nombre de destinataires du spam <= 10 : 30 € TTC
    - Nombre de destinataires du spam compris entre 10 et 50 : 60 € TTC
    - Nombre de destinataires du spam à partir de 50 : 300 € TTC
- 3ème envoi de spam :
  - Le Prestataire facture des frais de gestions selon les modalités suivantes :
    - Nombre de destinataires du spam <= 10 : 100 € TTC
    - Nombre de destinataires du spam compris entre 10 et 50 : 500 € TTC
    - Nombre de destinataires du spam à partir de 50 : 1000 € TTC

Les pénalités pour SPAMs sont facturées après constatation du SPAM par APICEM et information de l'utilisateur. La facturation est émise dans le mois suivant la détection et est payable selon les termes indiqués.

15 COMMUNICATIONS – NOTIFICATIONS - CONTACTS

Les communications et notifications entre le Prestataire et l'Utilisateur peuvent être effectuées par tout moyen, le Prestataire se réservant la possibilité de subordonner la tenue de certains échanges à l'envoi d'une lettre

recommandée papier avec accusé de réception ou par le biais d'un service de recommandé électronique répondant à des critères légaux.

Les Parties conviennent que les coordonnées de correspondance sont, en priorité, celles qui sont indiquées par l'Utilisateur lors de la procédure d'abonnement à la Solution APICRYPT® ou à l'occasion de la mise à jour par l'Utilisateur de ses coordonnées sur son espace personnel du site www.apicrypt.org en page de signature du présent contrat.

Conformément à l'exigence du référentiel de certification HDS, l'Utilisateur est sauf précision contraire de sa part et écrit, le point de contact qui doit être en mesure de désigner au Prestataire un professionnel de santé lorsque cela est nécessaire (exemples : accès aux données de santé, gestion des relations avec le patient, etc.).

16 FORMATION

Sur demande de l'Utilisateur, le Prestataire peut fournir, dans des conditions à définir par avenant, des prestations de formation.

De plus, les deux Parties s'autorisent la mise en œuvre d'actions de communication, ou de formation, conjointe en vue de sensibiliser et/ou former les Utilisateurs à un usage conforme de la Solution APICRYPT®

17 SOUS-TRAITANCE

Chaque fois que le Prestataire choisit de sous-traiter tout ou partie de la prestation, le Prestataire s'engage à respecter et à faire respecter un niveau équivalent de garantie au regard des obligations réglementaires pesant sur l'activité d'hébergement. Cet engagement est formalisé au travers d'accords contractuels (Plan d'Assurance Sécurité, contrat de confidentialités, etc.).

Dans le cadre de son contrat avec les éditeurs intégrant la solution APICRYPT®, le Prestataire définit précisément les relations avec ces derniers au travers de contrats dit d'intégration d'APICRYPT.

18 CONFIDENTIALITE

Le Prestataire ne communique sur ses utilisateurs que par le biais de la mise à jour de son Annuaire, les utilisateurs y figurant le sont avec leurs tacites accords, les informations communiquées ne le sont que dans un but d'usage de la Solution APICRYPT®. Les adresses de messagerie figurant sur l'annuaire sont uniquement les adresses permettant l'émission ou la réception de messages cryptés.

Les documents administratifs fournis par l'utilisateur ne font l'objet d'aucune transmission et sont conservés de façons sécurisées.

Les informations, contenus, et formes relatives aux méthodes, procédures, procédés techniques, bases de données, dessins, y compris toutes les informations qui seront transmises par les Parties entre elles seront considérées comme strictement confidentielles dans le cadre des discussions contractuelles entre le Prestataire et l'Utilisateur, ainsi que s'agissant de l'exécution du présent Contrat.

Chaque Partie s'engage à utiliser les informations confidentielles qu'elle reçoit, uniquement pour les besoins nécessaires à la mise en œuvre de la Solution APICRYPT®.

L'obligation de confidentialité se poursuit pendant une période de deux (2) ans après la cessation du présent contrat, pour quelque cause que ce soit.

CONFIDENTIALITE DES ÉLEMENTS SECRETS :

Les Éléments secrets sont personnels et confidentiels. Ils ne peuvent être changés que sur demande de l'Utilisateur ou à l'initiative du Prestataire sous réserve d'en informer préalablement l'Utilisateur.

L'Utilisateur s'engage à mettre tout en œuvre pour conserver secrets les Éléments secrets en sa possession et à ne pas les divulguer sous quelque forme que ce soit.

L'Utilisateur est entièrement responsable de l'utilisation des Éléments secrets et il est responsable de la garde des Éléments secrets qui lui sont remis. Il s'assurera qu'aucune autre personne non autorisée par le Prestataire n'a accès aux Éléments secrets.

De manière générale, l'Utilisateur assume la responsabilité de la sécurité des postes individuels d'accès à la Solution APICRYPT®. Dans l'hypothèse où il aurait connaissance de ce qu'une autre personne y accède, l'Utilisateur en informera le Prestataire sans délai et le confirmera par courrier recommandé.

En cas de perte ou de vol des Éléments secrets, l'Utilisateur utilisera la procédure mise en place par le Prestataire lui permettant de faire invalider ses Éléments secrets et de se faire adresser un nouveau jeu d'Éléments secrets. La procédure est décrite en Annexe C - 1.2 - Eléments Secrets.

19 PROPRIETE

L'association APICEM est titulaire de l'intégralité des droits de propriété intellectuelle liés à la conception, à la mise en œuvre et au fonctionnement du service de messagerie sécurisée en santé APICRYPT® et de tout outil technique utilisé dans ce cadre. Cette propriété inclut les codes sources des logiciels.

L'association APICEM a donné au Prestataire, la possibilité de déployer la Solution APICRYPT®, dans le respect de l'éthique qui lui a été confiée.

Le Prestataire ne peut modifier toute ou partie de la Solution APICRYPT® sans l'accord de l'association APICEM.

Le Prestataire concède à l'Utilisateur pour la durée du présent contrat un droit d'utilisation personnel, non exclusif et non transférable des outils et éléments logiciels de la Solution APICRYPT® pour les seuls besoins propres de l'Utilisateur dans les conditions du présent contrat. La durée de la licence concédée à l'Utilisateur prend effet à compter du jour de la mise en service de la prestation souscrite par l'Utilisateur.

Le Prestataire autorise l'Utilisateur à mentionner le nom commercial d'APICRYPT®, de son (ses) logo(s) et/ou signes distinctifs, de sa marque et autres désignations commerciales à titre de référence dans le cadre de supports de communication.

20 CESSION ET TRANSMISSION DU CONTRAT

Le présent contrat est conclu intuitu personae, les droits et obligations qui résultent de l'utilisation de la Solution APICRYPT®, étant personnels à l'Utilisateur, ne peuvent être transférés à quiconque, à aucun titre et sous quelque forme que ce soit par lui.

21 ASSURANCE

Le Prestataire déclare être titulaire d'une police d'assurance couvrant sa responsabilité civile, d'exploitation et professionnelle, contre les dommages corporels, matériels et immatériels dont elle aurait à répondre dans le cadre de l'exécution du contrat. Le Prestataire s'engage à conserver cette police d'assurance pendant toute la durée contrat et pourra communiquer à l'Utilisateur une attestation d'assurance sur simple demande.

22 STIPULATIONS DIVERSES

Si une ou plusieurs stipulations du Contrat devaient être tenues pour nuls ou non valides au titre d'une loi ou un règlement applicable en France ou déclarées tel par décision définitive d'une juridiction française, elles seront réputées non écrites, les autres stipulations du Contrat garderont toute leur force et leur portée.

Le fait que l'une ou l'autre des Parties ne se prévale pas à un moment donné de l'une des clauses prévues au présent Contrat ou qu'elle tolère l'inexécution de façon temporaire ou permanente des obligations de l'autre Partie ne peut être interprété comme valant renonciation à se prévaloir ultérieurement.

Le fait pour l'une ou l'autre des Parties de tolérer une inexécution ou une exécution imparfaite du présent Contrat ou, plus généralement, de tolérer tout acte, abstention ou omission de l'autre Partie non conforme aux stipulations du présent Contrat ne saurait conférer un droit quelconque à la Partie bénéficiant de cette tolérance.

Les Parties conviennent que le présent Contrat sera exécuté en toute indépendance réciproque, tant fonctionnelle que hiérarchique, notamment, en excluant tout lien de subordination entre les Parties.

En cas de difficulté d'interprétation entre l'intitulé du titre d'un article du présent Contrat et le contenu dudit article, seul le contenu de l'article devra être pris en compte.

Sont exclues du Contrat et peuvent donner lieu à facturation séparée et rédaction d'un avenant les prestations suivantes :

- Les prestations de formation ;
- Les développements spécifiques ;
- Et plus généralement toutes prestations n'entrant pas dans le champ du Contrat.

23 ELECTION DE DOMICILE

Les parties élisent domicile, sauf dérogation expresse convenue d'un commun accord, aux adresses de leur siège respectif.

ANNEXE A
-
DEFINITIONS

Les termes débutant par une majuscule au sein du Contrat, qu'ils soient utilisés au singulier ou au pluriel, auront la signification qui leur est donnée ci-après :

Solution APICRYPT® désigne les fonctions opérationnelles liées à la messagerie sécurisée en santé APICRYPT®.

Données désignent tout contenu d'un message électronique, quelle qu'en soit la nature, la taille et/ou le format, échangé via la Solution APICRYPT®, ce contenu ne pouvant être consulté que par l'émetteur et le destinataire du message.

Données Personnelles ou Données Personnelles de Santé :

Utilisateur(s) désigne une personne morale ou physique qui a recours aux services de la Solution APICRYPT®.

Composants APICRYPT® désigne les éléments logiciels et/ou matériels nécessaires au fonctionnement de la Solution APICRYPT®. Les API APICRYPT®, le middleware (ou compagnon,) APICRYPT®, les Clefs de chiffrement et les Clefs de signature ainsi que les matériels de type proxy sont des Composants APICRYPT®.

Éléments secrets désigne les éléments logiciels ou matériels permettant le chiffrement des messages et leurs signatures électroniques ainsi que les codes d'installation ou d'accès au compte personnel de l'Utilisateur.

Clef(s) de chiffrement désigne une donnée informatique unique destinée à réaliser une opération de chiffrement.

Clef(s) de signature désigne une donnée informatique unique destinée à réaliser une signature électronique. La clé de signature est fournie conjointement avec la clef de chiffrement.

Professionnels habilités désigne les professionnels ou les structures au sein desquelles ils exercent, identifiés par les référentiels nationaux d'identification des personnes physiques et des personnes morales des secteurs sanitaires, social et médico-social suivants :

- le répertoire partagé des professionnels de santé (RPPS) ;
- le répertoire ADELI (automatisation des listes) ;
- le répertoire FINESS (fichier d'identification nationale des établissements sanitaires et sociaux) ;
- le répertoire SIRENE (système informatique pour le répertoire des entreprises et de leurs établissements).

Ces professionnels peuvent également être identifiés par un référentiel d'identification local, c'est-à-dire propre à la structure dans laquelle le service de messagerie sécurisée de santé est déployé.

Le référencement d'une personne physique ou morale au sein d'un référentiel d'identification est réalisé à l'issue d'un processus de vérification de l'identité et de la fonction de la personne.

ANNEXE B
-
DESCRIPTIF DE LA SOLUTION APICRYPT®

1 DESCRIPTION DES SERVICES DE LA SOLUTION APICRYPT®

Le Prestataire met à disposition de l'Utilisateur la Solution APICRYPT® accessible sur ses serveurs en mode SaaS par le biais du réseau Internet. La Solution comprend les services et applicatifs suivants :

- Un accès aux serveurs de messagerie de la Solution APICRYPT®. Cet accès permet l'échange de messages sécurisés entre les utilisateurs de la Solution APICRYPT® ;
- Un annuaire accessible par navigateur web, protocole LDAP ou export, permet une recherche simple et ergonomique des professionnels de santé avec lesquels correspondre ;
- Un espace personnel accessible depuis le Site Internet www.apicrypt.org ;
- Des Composants APICRYPT® permettant l'utilisation de la Solution APICRYPT® ;
- Des Éléments Secrets permettant la sécurisation de la Solution et des échanges au travers de la Solution APICRYPT®.

1.1 COMPOSANTS APICRYPT®

Les Composants APICRYPT® sont destinés à être installés sur le poste de travail ou interfacés à la solution métier de l'Utilisateur afin de permettre l'usage des services de la Solution APICRYPT®.

Le Prestataire fournit un ensemble d'outils et documentations en fonction de la version d'APICRYPT® et du composant que l'Utilisateur souhaite utiliser :

- APICRYPT® V1 : client APImail pour différents systèmes d'exploitation (Windows, Mac) ;
- APICRYPT® V2 : Compagnon APICRYPT et client APImail pour différents systèmes d'exploitation (Windows, Mac).

L'installation des Composants APICRYPT® par l'Utilisateur se doit d'être faite conformément à la documentation associée au Composant.

L'Utilisateur reconnaît avoir pris connaissance de ces préconisations et déclare les accepter sans réserve.

1.2 ELEMENTS SECRETS

Les Éléments secrets sont destinés à réserver l'accès à la Solution APICRYPT® aux Utilisateurs, à protéger l'intégrité et la disponibilité de la Solution, ainsi que l'intégrité, la disponibilité et la confidentialité des Données telles que transmises par les Utilisateurs.

Les Éléments Secrets sont constitués :

- Des clefs de chiffrements APICRYPT® personnelles et communes ;
- De la clef de signature personnelle ;
- Du code de déchiffrement et d'installation des clefs de chiffrements APICRYPT® V2 ;
- Des identifiants d'accès au compte personnel sur le site www.apicrypt.org ou à la Solution APICRYPT®.

La procédure d'obtention de renouvellement ou de déclaration de perte ou vol des Éléments Secrets est détaillée ci-après.

L'Utilisateur s'engage à ne pas utiliser les Éléments Secrets qui lui sont attribués à d'autres fins que celles listées précédemment et, en tout état de cause, à respecter la Charte d'utilisation de la messagerie sécurisée en santé APICRYPT®.

1.2.1 OBTENTION

Les Éléments Secrets sont adressés automatiquement à l'Utilisateur lors de la souscription de son abonnement à la Solution APICRYPT®. Les Éléments Secrets sont adressés par courrier postal. Il est nécessaire de procéder à l'installation des clefs et outils contenus dans le support amovible APICRYPT® dans les plus brefs délais afin de pouvoir déceler une éventuelle erreur technique (support CD ou USB défaillant, fichier non lisible par l'ordinateur, etc.). Le support d'installation des clefs contient la documentation d'utilisation associée.

1.2.2 RENOUVELLEMENT

Le renouvellement des Éléments Secrets se fait automatiquement dès acceptation du renouvellement du contrat d'abonnement à la Solution APICRYPT® et en tout état de cause avant la fin de l'année en cour. Ces Éléments Secrets sont adressés selon les mêmes modalités que celles décrites précédemment. Il est nécessaire de procéder à l'installation de ces clefs dans les plus brefs délais afin de pouvoir déceler une éventuelle erreur technique (support CD ou USB défaillant, fichier non lisible par l'ordinateur, etc.). Le support d'installation des clefs contient la documentation associée.

1.2.3 PERTE OU VOL

L'Utilisateur informera dans les plus brefs délais le Prestataire de toute compromission, toute perte ou tout vol de ses Éléments Secrets par téléphone au numéro suivant : 03 28 63 00 65 ou par e-mail à infoapicrypt@apicrypt.org et par courrier postal daté et signé envoyé à l'adresse suivante : APICEM SARL, 3 route de Bergues – CS 20007 – 59412 Coudekerque-Branche Cedex.

Les Éléments Secrets déclarés corrompus, perdus ou volés seront alors invalidés par le Prestataire et un nouveau support amovible contenant de nouveaux Éléments Secrets est adressé par courrier postal urgent aux Utilisateurs.

1.3 ESPACE PERSONNEL

L'ensemble des éléments relatifs au compte utilisateur principal ou secondaire est consultable dans la rubrique « mon compte » du site www.apicrypt.org.

L'Utilisateur peut personnaliser ses éléments d'identification en s'adressant au service technique du Prestataire.

L'espace personnel permet à l'Utilisateur de configurer sa Solution APICRYPT® et notamment les options d'interopérabilité avec l'Espace de confiance MSSanté.

1.4 ACCES AUX SERVEURS DE MESSAGERIE

Cet accès offre à l'Utilisateurs, la possibilité d'échanger des messages avec des Utilisateurs de la Solution APICRYPT®.

Pour pouvoir utiliser la Solution APICRYPT®, tout Utilisateur devra ouvrir un compte de messagerie auprès du Prestataire en s'abonnant à la messagerie sécurisée en santé APICRYPT® et procéder à l'installation des Composants et Éléments Secrets adaptés à son utilisation.

L'émetteur décide seul des destinataires des messages qu'il fait transiter via la Solution APICRYPT®. Celle-ci permet la transmission de données médicales nominatives sur le réseau Internet.

La plateforme de message sécurisée APICRYPT® ne stocke que provisoirement les messages jusqu'à leur relève par tous les destinataires de ces messages. La durée de stockage du contenu des messages est donc limitée au temps nécessaire de traversée et de stockage des équipements actifs des réseaux sans mise en œuvre de traitement applicatif autre que la messagerie.

1.5 ANNUAIRE

L'annuaire des Utilisateurs de la Solution APICRYPT® est consultable et téléchargeable sur le site www.apicrypt.org. Cet annuaire offre aux Utilisateurs de multiples critères de recherche afin qu'ils puissent identifier leurs destinataires avec précision.

L'annuaire est aussi disponible au travers des composants APICRYPT® ou de la solution métier de l'Utilisateur lorsque celle-ci intègre APICRYPT®.

ANNEXE C
-
QUALITE

1 ORGANISATION DU PRESTATAIRE

Afin de permettre les échanges sécurisés, le Prestataire dispose d'un site « maître ».

Le personnel de ce site est composé de (outre l'équipe administrative chargée de la gestion des dossiers financiers et du personnel) :

- Un Directeur technique ;
- Un Directeur d'exploitation ;
- Un Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- Un RSSI adjoint.

Ces quatre fonctions au moins, assurent des astreintes techniques permettant la continuité de service 24/24 - 7j/7.

Afin de répondre aux questions techniques courantes des utilisateurs, un service d'assistance technique assure une permanence de service de 8 heures à 19 heures du lundi au vendredi et une permanence le samedi matin de 9 heures à midi (hors jours fériés).

Le Prestataire dispose de lignes numériques, de lignes analogiques et également de liaisons satellites (avec FAI différent) permettant d'assurer une continuité de service.

2 DISPONIBILITE DE LA SOLUTION APICRYPT®

Le Prestataire dispose d'un site sécurisé de secours. La communication entre les sites est constante. En cas d'incident majeur ou de cas de force majeure, le service assistance technique peut être déplacé dans un délai n'excédant pas quatre heures, de plus en cas d'extrême urgence ou de consignes préfectorales de confinement, le service assistance technique est également déplaçable de façon sécurisée.

La continuité d'activité est assurée par la mise en œuvre d'une politique de sauvegarde et de réplication de l'architecture de la Solution APICRYPT®.

3 GARANTIES ET MAINTENANCE

Le Prestataire prend en charge la maintenance corrective et évolutive des Composants et de la Solution APICRYPT®.

Une prestation de support par téléphone permettant de traiter les anomalies est accessible à l'Utilisateur du lundi au vendredi inclus, de 9h à 19h, hors jours fériés. Les signalements d'anomalie doivent être confirmés par e-mail au Prestataire sans délai et accompagnés de tout élément permettant au Prestataire de reproduire les anomalies. Le Prestataire procède au diagnostic de l'anomalie et met ensuite en œuvre sa correction.

Les activités de maintenance de la Solution APICRYPT® sont planifiées pour être le plus transparentes possible pour les Utilisateurs de la Solution. Lorsqu'un arrêt de la Solution est décidé pour une activité de maintenance, le Prestataire communique l'information par tout moyen aux Utilisateurs.

4 ASSISTANCE TECHNIQUE UTILISATEURS

Le Prestataire s'oblige à assurer une prestation d'aide et d'assistance à l'installation et à l'utilisation de la Solution APICRYPT® au bénéfice des Utilisateurs de la Solution APICRYPT®.

Cette prestation sera assurée, sur appel au numéro 03 28 63 00 65, par les équipes du Prestataire pendant toute la durée de l'abonnement de l'Utilisateur, du lundi au vendredi inclus, de 8h à 19h et le samedi de 9h à 12h, hors jours fériés.

Cette prestation sera limitée à une obligation de moyens.

ANNEXE D
-
CHARTE DE BON USAGE DE LA SOLUTION APICRYPT®

LES ELEMENTS DE LA CHARTE, CI-APRES, SONT A TRANSMETTRE AUX UTILISATEURS FINAUX DE LA SOLUTION APICRYPT®

L'objectif de cette charte est de rappeler les quelques règles à respecter pour simplifier les échanges avec vos confrères. Les courriers que vous envoyez sont destinés à être intégrés dans les dossiers médicaux de vos correspondants. Or, les outils de réception sont très divers et pour éviter les erreurs de transmission, il convient de respecter certains principes.

JE ME LIMITE AUX COMMUNICATIONS PROFESSIONNELLES

La messagerie électronique sécurisée sert avant tout à intégrer les données dans le dossier médical, c'est sa fonction première et exclusive. Les communications privées n'ont vocation ni à être sécurisées ni intégrées dans un logiciel métier.

JE PRIVILEGIE LA TRANSMISSION DE L'INFORMATION DANS LE CORPS DU MESSAGE

Il faut éviter de transmettre l'information sous forme de document joint, car cela peut être source d'erreur. Il est important que le texte apparaisse directement dans le corps du message, car seuls quelques rares logiciels médicaux travaillent efficacement avec des documents joints.

JE NE FAIS PAS D'ENVOIS GROUPES DE TYPE ANNONCE, INVITATION, ETC.

Utiliser APICRYPT® pour faire des envois groupés à des Apicrypteurs est proscrit. Ce genre de message peut être assimilé à un spam dans la mesure où il s'agit d'un message non désiré et qui risque de bloquer les logiciels de vos correspondants.

JE REMPLIS CORRECTEMENT L'EN-TETE DU MESSAGE (EN-TETE DIT H.P.R.I.M.)

Il faut indiquer au minimum les nom, prénom et date de naissance du patient. Ces informations permettront une intégration facile dans les dossiers médicaux respectifs.

JE PENSE A VERIFIER MES MESSAGES

Les messages doivent être vérifiés avant envoi même s'il ne s'agit que de l'envoi de comptes rendus.