Aida.

PROTECTION DES DONNÉES · NLPD

Contrat de sous-traitance de données personnelles

conclu en application de l'**art. 9 LPD** entre le Client (le « **Responsable du traitement** ») et **Aida Medical SA** (le « **Sous-traitant** »),

Campus Biotech Innovation Park · Avenue de Sécheron 15 · 1202 Genève · IDE CHE-458.981.803

VERSION	BASE LÉGALE	DONNÉES TRAITÉES	LIEU DU TRAITEMENT
1.0 En vigueur dès le 30 octobre 2026	**Art. 9 LPD · OPDo** nLPD du 25 septembre 2020	**Données sensibles** Données sur la santé, art. 5 let. c LPD	**Suisse uniquement** Hébergement Infomaniak, ISO 27001

Les Annexes 1 à 3 font partie intégrante du contrat. Point de contact protection des données : legal@aida.med.

Le Responsable du traitement utilise les Services d'Aida Medical SA conformément aux Conditions générales SaaS et à l'Offre (ensemble, le « **Contrat principal** »). Dans ce cadre, le Sous-traitant traite pour le compte du Responsable des données personnelles, dont des **données sensibles sur la santé** de patients. Le présent contrat de sous-traitance (le « **CST** ») règle ce traitement conformément à la loi fédérale sur la protection des données (LPD) et à son ordonnance (OPDo). Il fait partie intégrante du Contrat principal et **prévaut sur celui-ci pour toute question relative à la protection des données**.

Art. 01 Définitions

1.1 Les termes « données personnelles », « données sensibles », « traitement », « responsable du traitement », « sous-traitant », « violation de la sécurité des données » et « personne concernée » ont le sens que leur donne l'art. 5 LPD.

1.2 « **Données** » désigne les données personnelles traitées par le Sous-traitant pour le compte du Responsable au moyen des Services, telles que décrites à l'**Annexe 1**. Les termes en majuscule non définis ici ont le sens du Contrat principal.

Art. 02 Objet, nature, finalité et durée du traitement

2.1 Le Sous-traitant traite les Données exclusivement pour fournir les Services au Responsable : transcription en direct de la consultation en texte (sans enregistrement audio), génération de projets de notes de consultation, propositions de codage (ICD-10, TARDOC) ou de devis au tarif dentaire, structuration des données cliniques, transmission au DPI et, le cas échéant, à Médident, hébergement, sauvegarde, journalisation et support. La description détaillée du traitement figure à l'**Annexe 1**.

2.2 Le CST s'applique pendant toute la durée du Contrat principal et, au-delà, jusqu'à l'achèvement de la restitution et de l'effacement des Données conformément à l'art. 11.

Art. 03 Instructions du Responsable

3.1 Le Sous-traitant ne traite les Données que sur instructions documentées du Responsable. Constituent des instructions documentées : le Contrat principal et le présent CST, la configuration des Services effectuée par le Responsable, ainsi que toute instruction écrite ultérieure raisonnable.

3.2 Si le Sous-traitant estime qu'une instruction viole le droit de la protection des données, il en informe le Responsable sans délai et peut suspendre l'exécution de l'instruction concernée jusqu'à sa confirmation ou sa modification.

3.3 Le Sous-traitant ne traite aucune Donnée pour son propre compte ou celui de tiers. L'établissement de statistiques agrégées et anonymisées de manière irréversible, tel que prévu par le Contrat principal, n'est pas un traitement de données personnelles.

Art. 04 Confidentialité et secret professionnel

4.1 Le Sous-traitant limite l'accès aux Données aux personnes qui en ont besoin pour exécuter le Contrat principal. Ces personnes sont liées par des engagements de confidentialité écrits et formées à la protection des données.

4.2 Les personnes autorisées sont informées qu'elles interviennent en qualité d'auxiliaires d'un professionnel soumis au secret médical et qu'elles sont elles-mêmes soumises au secret (art. 321 CP) ainsi qu'au devoir de discrétion de l'art. 62 LPD.

4.3 Ces obligations de confidentialité survivent à la fin du CST.

Art. 05 Sécurité du traitement

5.1 Le Sous-traitant met en œuvre et maintient les mesures techniques et organisationnelles décrites à l'**Annexe 2**, appropriées au risque élevé que présente le traitement de données sur la santé, conformément aux art. 7 et 8 LPD et aux exigences minimales de l'OPDo (confidentialité, disponibilité, intégrité, traçabilité).

5.2 Le Sous-traitant peut adapter ces mesures à l'évolution de l'état de la technique, pour autant que le niveau de protection convenu ne soit pas réduit.

5.3 Le traitement respecte les principes de protection des données dès la conception et par défaut (art. 7 LPD), notamment la minimisation des données, l'absence de tout enregistrement audio et la limitation des durées de conservation décrites à l'Annexe 1.

Art. 06 Sous-traitants ultérieurs

6.1 Conformément à l'art. 9 al. 3 LPD, le recours à un sous-traitant ultérieur requiert l'autorisation préalable du Responsable. Le Responsable autorise de manière générale les sous-traitants ultérieurs énumérés à l'**Annexe 3**.

6.2 Le Sous-traitant informe le Responsable par écrit (courriel admis) de tout ajout ou remplacement envisagé au moins **trente jours** avant sa mise en œuvre. Le Responsable peut s'y opposer par écrit, pour de justes motifs liés à la protection des données, dans les trente jours suivant l'information.

6.3 En cas d'opposition et à défaut de solution raisonnable, le Responsable peut résilier sans pénalité les Services concernés par le changement, pour la date de mise en œuvre de celui-ci.

6.4 Le Sous-traitant impose contractuellement à chaque sous-traitant ultérieur des obligations au moins équivalentes à celles du présent CST, y compris la localisation du traitement, et répond des actes de ses sous-traitants ultérieurs comme des siens propres.

Art. 07 Lieu du traitement et communication à l'étranger

ENGAGEMENT DE LOCALISATION

L'ensemble du traitement des Données (hébergement, traitement par les systèmes d'intelligence artificielle, sauvegardes, journaux et support) est effectué **exclusivement en Suisse**. Les accès d'administration sont nominatifs, journalisés et limités au territoire suisse.

7.1 Aucune Donnée n'est communiquée à l'étranger sans l'accord écrit préalable du Responsable et sans le respect des conditions des art. 16 ss LPD (État assurant un niveau de protection adéquat ou garanties appropriées, telles que des clauses contractuelles types reconnues par le PFPDT).

Art. 08 Assistance au Responsable

8.1 Droits des personnes concernées. Le Sous-traitant transmet sans délai au Responsable toute demande d'une personne concernée qui lui parviendrait directement (droit d'accès de l'art. 25 LPD, remise ou transmission des données de l'art. 28 LPD, rectification, effacement ou opposition de l'art. 32 LPD) et n'y répond pas lui-même, sauf instruction contraire. Il fournit au Responsable, par des mesures techniques et organisationnelles appropriées (fonctions d'export, de rectification et d'effacement de la Plateforme), l'assistance raisonnablement nécessaire pour y donner suite dans les délais légaux.

8.2 Analyse d'impact et consultation. Le Sous-traitant fournit au Responsable les informations raisonnablement nécessaires à la réalisation d'une analyse d'impact relative à la protection des données (art. 22 LPD) et, le cas échéant, à la consultation du PFPDT (art. 23 LPD).

8.3 Devoir d'information. Le Sous-traitant met à la disposition du Responsable les informations utiles à l'exécution de son devoir d'information envers les personnes concernées (art. 19 à 21 LPD), notamment la description du traitement (Annexe 1) et la liste des sous-traitants ultérieurs (Annexe 3). Un modèle d'information aux patients est fourni avec la documentation des Services.

Art. 09 Violations de la sécurité des données

9.1 Le Sous-traitant annonce au Responsable toute violation de la sécurité des données au sens de l'art. 5 let. h LPD **dans les meilleurs délais** après en avoir eu connaissance, au plus tard dans les **24 heures**.

9.2 L'annonce décrit, dans la mesure des informations disponibles : la nature de la violation ; les catégories et le nombre approximatif de personnes concernées et de Données touchées ; les conséquences probables ; les mesures prises ou proposées pour y remédier et en atténuer les effets ; un point de contact. Les informations manquantes sont communiquées dès qu'elles sont disponibles.

9.3 Le Sous-traitant documente les violations et leur traitement, prend sans délai les mesures de confinement et de correction nécessaires et assiste le Responsable pour l'annonce au PFPDT et, le

cas échéant, l'information des personnes concernées (art. 24 LPD). L'annonce d'une violation ne vaut pas reconnaissance de responsabilité.

Art. 10 Preuve de conformité et audit

10.1 Le Sous-traitant tient la documentation permettant de démontrer le respect du présent CST : registre des activités de traitement (art. 12 LPD), description des mesures de sécurité, certifications et attestations de son hébergeur, synthèses des tests d'intrusion.

10.2 Sur demande écrite, au plus une fois par année civile, ou sans limitation après une violation significative, le Responsable peut faire vérifier le respect du CST, par lui-même ou par un tiers qualifié non concurrent du Sous-traitant, moyennant un préavis de trente jours, pendant les heures ouvrées, sous engagement de confidentialité et sans accès aux données d'autres clients.

10.3 Les frais de l'audit sont à la charge du Responsable, sauf si l'audit révèle un manquement significatif du Sous-traitant.

Art. 11 Restitution et effacement des Données

11.1 À la fin du Contrat principal, le Sous-traitant restitue au Responsable l'intégralité des Données, y compris les journaux pertinents, dans les **trente jours**, dans des formats ouverts, structurés et documentés.

11.2 Après confirmation de la restitution, le Sous-traitant efface toutes les copies des Données, y compris chez ses sous-traitants ultérieurs. Les sauvegardes sont écrasées par rotation au plus tard **nonante jours** après la restitution ; jusqu'à leur effacement, elles restent protégées par le présent CST et ne font l'objet d'aucune restauration, sauf obligation légale. Le Sous-traitant fournit une **attestation écrite d'effacement**.

11.3 Si une obligation légale impose au Sous-traitant de conserver certaines Données, il en informe le Responsable, limite la conservation à ce qui est exigé et maintient les protections du présent CST.

Art. 12 Responsabilité

12.1 La responsabilité des parties est régie par l'art. 13 des Conditions générales SaaS. Chaque partie répond des violations de la LPD qui lui sont imputables au regard de son rôle de responsable du traitement, respectivement de sous-traitant.

12.2 Demeurent réservées les sanctions prévues par les art. 60 ss LPD, qui frappent personnellement les personnes physiques responsables.

Art. 13 Durée, fin et dispositions finales

13.1 Le CST prend effet avec le Contrat principal et prend fin avec l'achèvement des opérations de l'art. 11. Les art. 4, 9, 11 et 12 survivent à sa fin dans la mesure nécessaire.

13.2 Toute modification du CST requiert la forme écrite. En cas de contradiction avec le Contrat principal, le CST prévaut pour les questions de protection des données.

13.3 Le CST est soumis au droit matériel suisse ; le for exclusif est à Genève, sous réserve des fors impératifs.

SIGNATURES

Fait en deux exemplaires originaux. Les Annexes 1 à 3 font partie intégrante du présent contrat. Pour toute question relative à la protection des données : **legal@aida.med**.

LE RESPONSABLE DU TRAITEMENT

Raison sociale / Nom :

_____

Lieu et date

Nom, fonction et signature

LE SOUS-TRAITANT

Aida Medical SA, Genève

Lieu et date

Nom, fonction et signature

ANNEXE 1

Description du traitement

Objet	Fourniture des Services Aida : assistance administrative et documentaire à la consultation médicale ou dentaire.
Nature et opérations	Collecte par transcription en direct de la parole en texte (**aucun enregistrement audio n'est effectué ni conservé**) ; génération de projets de notes de consultation ; propositions de codage ICD-10 et TARDOC ou de devis au tarif dentaire ; structuration des données cliniques ; transmission au DPI du Responsable et, le cas échéant, à Médident ; hébergement ; sauvegarde ; journalisation ; support ; effacement.
Finalités	Documentation médicale et administrative des consultations du Responsable ; préparation du codage tarifaire ou du devis ; sécurité et traçabilité du traitement.
Catégories de personnes concernées	Patientes et patients du Responsable ; professionnels de la santé et collaborateurs du Responsable (Utilisateurs autorisés) ; le cas échéant, tiers mentionnés au cours d'une consultation (p. ex. proches).
Catégories de Données	Identité et coordonnées des patients ; **données sur la santé** (anamnèse, constatations, diagnostics, traitements, codes), soit des données sensibles au sens de l'art. 5 let. c LPD ; données administratives et tarifaires, y compris la classe de payeur ; transcriptions écrites des consultations ; données d'identification et d'utilisation des Utilisateurs autorisés ; journaux techniques.
Durées de conservation	Audio : aucun ; le flux audio est transcrit en temps réel et n'est jamais stocké. Transcriptions, notes et données structurées : tant que le Responsable les conserve dans les Services. Journaux d'accès : douze mois. Sauvegardes : trente jours (rotation).
Lieu du traitement	Suisse exclusivement (art. 7 CST).

ANNEXE 2

Mesures techniques et organisationnelles

1 · Hébergement et sécurité physique

- Données de production, journaux et sauvegardes hébergés exclusivement en Suisse, dans les centres de données d'Infomaniak SA, certifiés **ISO 27001** (label Swiss Hosting), avec redondance géographique.
- Contrôles d'accès physiques, alimentation et refroidissement redondants assurés par l'hébergeur.

2 · Chiffrement

- Chiffrement des Données au repos (**AES-256**) et en transit (**TLS 1.3**) ; sauvegardes chiffrées.
- Gestion des clés sur modules matériels (HSM) certifiés **FIPS 140-2 niveau 3**.

3 · Identités et contrôle des accès

- Authentification forte (MFA) pour l'ensemble des comptes ; gestion des rôles (RBAC) alignée sur les fonctions du cabinet ; principe du moindre privilège et revue périodique des droits.
- Accès d'administration nominatifs, journalisés et limités au territoire suisse.

4 · Traçabilité et journalisation

- Journalisation des lectures, créations, modifications, exports et suppressions de Données, conformément à l'OPDo.
- Journaux conservés douze mois, avec copie externalisée immuable garantissant leur disponibilité et leur intégrité.

5 · Sécurité des réseaux et des systèmes

- Cloisonnement des réseaux et des environnements ; supervision et alertes ; gestion des vulnérabilités et des correctifs.
- Tests d'intrusion annuels réalisés par un tiers indépendant ; durcissement des systèmes.

6 · Développement et minimisation

- Protection des données dès la conception et par défaut (art. 7 LPD) : seules les données nécessaires à chaque finalité sont traitées.
- Environnements de développement, de test et de production séparés ; aucune Donnée de production en développement ou en test ; revues de code.
- **Aucun stockage de l'audio** : la parole est transcrite en temps réel et seul le texte est persisté ; procédures d'effacement documentées.

7 · Continuité et disponibilité

- Sauvegardes quotidiennes chiffrées, conservées trente jours ; objectifs de reprise **RPO ≤ 24 h** et **RTO ≤ 4 h**.
- Plans de continuité et de reprise testés annuellement ; mode dégradé : le DPI du Responsable fonctionne sans les Services.

8 · Organisation et personnel

- Politique de sécurité de l'information ; registre des activités de traitement (art. 12 LPD) ; point de contact protection des données : **legal@aida.med**.
- Engagements de confidentialité écrits ; formation et sensibilisation régulières du personnel au secret médical et à la protection des données.
- Processus de gestion des incidents : détection et qualification sous quatre heures ouvrées, confinement, analyse post-incident et mesures correctives ; registre des incidents.

ANNEXE 3

Sous-traitants ultérieurs autorisés

Liste des sous-traitants ultérieurs autorisés au sens de l'art. 6 du CST, à la date de la version 1.0 :

SOUS-TRAITANT	SIÈGE	PRESTATION	LIEU DU TRAITEMENT
Infomaniak SA	Genève, Suisse	Hébergement cloud et centres de données (données chiffrées), infrastructure de calcul pour le traitement IA	Suisse

Aucun autre sous-traitant ultérieur n'accède aux Données. Toute modification de cette liste suit la procédure d'information et d'opposition prévue à l'art. 6 du CST. La version à jour est disponible sur demande auprès de **legal@aida.med**.