Accord de traitement des données (ATD) medidux™

entre

[Nom du Client]
[Adresse]
[NPA, localité]
Suisse

ci-après le « Client »

et

mobile Health AG
Mühlebachstrasse 43
8008 Zurich
Suisse

ci-après le « Sous-traitant »

ensemble, les « Parties »

Sommaire

1. Objet de l'accord 3
2. Rôles des Parties 3
3. Objet, nature et finalités du traitement 3
4. Catégories de données personnelles 4
5. Catégories de personnes concernées 5
6. Durée du traitement 5
7. Instructions du Client 5
8. Obligations du Client 5
9. Obligations du Sous-traitant 6
10. Confidentialité 6
11. Lieu du traitement 6
12. Sous-traitants ultérieurs 6
13. Mesures techniques et organisationnelles 7
14. Notification des violations de données personnelles 7
15. Assistance pour l'exercice des droits des personnes concernées 8
16. Assistance concernant les obligations de protection des données 8
17. Droits d'audit 8
18. Restitution et suppression à la fin des relations contractuelles 8
19. Utilisation de données anonymisées ou agrégées 9
20. Responsabilité 9
21. Dispositions finales 9

1. Objet de l'accord

Le présent accord de traitement des données régit les droits et obligations des Parties concernant le traitement de données personnelles par le Sous-traitant pour le compte du Client dans le cadre de l'utilisation de medidux™.

Il complète l'offre, les Conditions générales / Conditions d'utilisation de medidux™ SaaS ainsi que tout autre accord entre les Parties.

En cas de divergence entre le présent accord et les documents susmentionnés, le présent accord prévaut.

2. Rôles des Parties

Dans le cadre de l'utilisation de medidux™, le Client détermine les finalités et les moyens du traitement des données des patients et d'autres données personnelles et agit à ce titre en qualité de responsable du traitement.

Le Sous-traitant traite les données personnelles pour le compte du Client et conformément à ses instructions, sauf lorsqu'il assume exceptionnellement ses propres obligations légales ou ses propres responsabilités.

3. Objet, nature et finalités du traitement

Le traitement porte sur la mise à disposition technique, le stockage, la transmission, l'affichage, l'assistance, la sauvegarde et l'évaluation des données dans le cadre de l'utilisation convenue de medidux™.

Le traitement est effectué notamment aux fins suivantes :

- mise à disposition de la plateforme medidux™,
- collecte structurée d'informations relatives aux patients,
- affichage de données sur les symptômes, paramètres vitaux, médicaments, évolution, questionnaires, laboratoire et diagnostic,
- traitement, affichage, transmission et stockage de données de laboratoire et de diagnostic si cela est prévu dans les prestations convenues, au moyen de saisies manuelles, de téléversements ou d'interfaces connectées,
- soutien à la communication et à la prise en charge par le Client,
- traitement, affichage, transmission et stockage de données de génomique, pathologie moléculaire, biomarqueurs, formulaires, registres, études, boards et consultations si cela est prévu dans les prestations convenues, au moyen de saisies manuelles, de téléversements ou d'interfaces connectées,
- administration technique,
- assistance,
- analyse des erreurs,
- sauvegarde des données,
- mise à disposition de rapports ou d'exports si convenu,
- réalisation de processus d'étude ou de soins convenus.

4. Catégories de données personnelles

Le traitement peut notamment porter sur les catégories suivantes de données personnelles (ci-après également les « Données traitées ») :

- données de base des patients,
- coordonnées,
- date de naissance,
- sexe,
- numéros de patients ou identifiants internes,
- données de santé,
- diagnostics,
- symptômes,
- degrés de gravité,
- bien-être,
- paramètres vitaux,
- poids,
- pression artérielle,
- pouls,
- saturation en oxygène,
- température,
- glycémie,
- données ECG, si utilisées,
- valeurs de CRP, si utilisées,
- données de laboratoire et valeurs diagnostiques si elles sont prévues dans les prestations concernées,
- résultats de laboratoire, paramètres, plages de référence, dates de prélèvement, dates des constatations et métadonnées associées traités via des interfaces, des saisies manuelles, des téléversements ou des systèmes connectés,
- données de génomique, de pathologie moléculaire et relatives aux biomarqueurs si elles sont prévues dans les prestations concernées,
- données de formulaires, formulaires de saisie structurés, formulaires de documentation médicale et informations de validation ou de statut associées,
- données relatives aux réunions médicales interdisciplinaires, consultations spécialisées et boards, notamment résumés de cas, questions, recommandations, décisions, procès-verbaux et informations médicales associées, si cela est prévu dans les prestations concernées,
- données de registres et d'études, notamment données d'inclusion, de suivi, de résultats et de documentation liées aux registres, si cela est prévu dans les prestations concernées,
- médicaments,
- événements thérapeutiques,
- effets secondaires,
- réponses aux questionnaires,
- communications,
- notes de traitement ou de suivi,
- informations liées aux études,
- état de santé,
- données techniques d'utilisation,
- données de journalisation,
- données relatives aux utilisateurs et aux autorisations.

Le traitement concret des données dépend de l'étendue des prestations convenue entre les Parties, de la configuration du système et des interfaces éventuellement convenues.

5. Catégories de personnes concernées

Les personnes concernées peuvent notamment être :

- les patients du Client,
- les participants à des études,
- les utilisateurs du Client,
- les professionnels de santé,
- le personnel infirmier,
- le personnel d'étude,
- les collaborateurs administratifs,
- les administrateurs techniques.

6. Durée du traitement

Le traitement commence à la prise d'effet de la relation de base entre les Parties (voir ch. 1) ou au début de l'utilisation de medidux™, selon l'événement qui survient en premier.

Il prend fin à la fin de la relation de base, sauf si des obligations légales de conservation, des intérêts légitimes, des instructions du Client ou des délais de transition technique s'y opposent.

7. Instructions du Client

Le Sous-traitant traite les Données traitées uniquement conformément aux instructions du Client, pour autant qu'elles soient documentées par écrit ou électroniquement.

Constituent notamment des instructions :

- le présent accord,
- l'offre / le formulaire de commande ainsi que tout autre document régissant la relation de base entre les Parties,
- la configuration convenue du système,
- les instructions du Client communiquées par écrit ou documentées électroniquement.

Le Sous-traitant informe le Client s'il estime qu'une instruction enfreint les règles de protection des données. Il n'est pas tenu de procéder à un examen juridique complet.

8. Obligations du Client

Le Client veille à ce que :

- le traitement des données soit licite,
- les patients soient informés de manière appropriée,
- les consentements requis soient obtenus,
- toute levée nécessaire du secret médical soit obtenue,
- l'utilisation de medidux™ respecte les règles internes,
- seules des personnes autorisées aient accès aux données,

- les autorisations soient correctement attribuées et mises à jour,
- les droits des personnes concernées soient respectés,
- les obligations de documentation médicale et légale soient respectées.

Le Client est responsable de l'exactitude, de l'admissibilité et de la licéité des données saisies par lui-même, ses utilisateurs ou les patients.

9. Obligations du Sous-traitant

Le Sous-traitant s'engage à :

- traiter les Données traitées uniquement aux fins convenues,
- garder les Données traitées confidentielles,
- n'accorder l'accès qu'aux personnes qui en ont besoin pour leurs tâches,
- soumettre les personnes ayant accès aux Données traitées à une obligation de confidentialité,
- mettre en œuvre des mesures techniques et organisationnelles appropriées,
- assister raisonnablement le Client dans l'exercice des droits des personnes concernées,
- signaler sans délai les violations de données personnelles,
- ne faire appel à des sous-traitants qu'en conformité avec le présent accord,
- restituer ou supprimer les Données traitées après la fin du contrat selon les instructions, sauf obligation légale contraire.

10. Confidentialité

Le Sous-traitant veille à ce que toutes les personnes ayant accès aux Données traitées soient soumises à une obligation légale ou contractuelle de confidentialité.

L'obligation de confidentialité perdure après la fin de la relation contractuelle.

11. Lieu du traitement

Les Données traitées sont en principe stockées en Suisse, sauf accord contraire.

Un traitement ou un accès depuis des États n'offrant pas un niveau adéquat de protection des données n'est autorisé que si les conditions requises sont remplies, notamment la mise en place de garanties appropriées telles que des clauses contractuelles types ou des mesures équivalentes.

12. Sous-traitants ultérieurs

Le Sous-traitant peut faire appel à des sous-traitants ultérieurs si cela est nécessaire à la fourniture des prestations.

Le Sous-traitant veille à ce que les sous-traitants ultérieurs soient liés contractuellement par des obligations de protection des données, de sécurité des données et de confidentialité.

Le Client est informé de manière appropriée des changements importants concernant les sous-traitants ultérieurs.

Si le Client s'oppose à un nouveau sous-traitant pour un motif important lié à la protection des données dans un délai raisonnable, les Parties recherchent une solution appropriée. À défaut de solution, le Client peut résilier la partie des prestations concernée.

Le Sous-traitant répond du respect par ses sous-traitants ultérieurs des obligations de protection des données comme de son propre comportement.

13. Mesures techniques et organisationnelles

Le Sous-traitant prend des mesures techniques et organisationnelles appropriées pour protéger les Données traitées.

Ces mesures concernent notamment :

- le contrôle des accès,
- le contrôle des entrées,
- la gestion des utilisateurs et des autorisations,
- le chiffrement, dans la mesure appropriée,
- la journalisation,
- les processus de sauvegarde et de restauration,
- la protection contre les accès non autorisés,
- la confidentialité,
- l'intégrité,
- la disponibilité,
- la résilience des systèmes,
- les processus de détection et de traitement des incidents de sécurité,
- la transmission sécurisée des données,
- la séparation des ensembles de données si nécessaire,
- le contrôle et l'amélioration réguliers des mesures de sécurité.

Le Sous-traitant peut adapter les mesures de sécurité à condition de ne pas réduire sensiblement le niveau de sécurité.

14. Notification des violations de données personnelles

Le Sous-traitant informe le Client sans délai dès qu'il a connaissance d'une violation de sécurité entraînant la destruction, la perte, la modification, la divulgation ou l'accès non autorisés, accidentels ou illicites aux Données traitées.

Dans la mesure où elles sont disponibles, la notification contient :
• la nature de la violation,
• les catégories de données concernées,
• les catégories de personnes concernées,
• le nombre approximatif de personnes concernées,
• les conséquences possibles,
• les mesures prises ou proposées,
• le point de contact pour toute question complémentaire.

Les informations peuvent être communiquées ultérieurement si elles ne sont pas immédiatement disponibles.

15. Assistance pour l'exercice des droits des personnes concernées

Si une personne concernée s'adresse directement au Sous-traitant pour exercer ses droits, celui-ci transmet la demande au Client dans la mesure où elle porte sur les Données traitées.

Le Sous-traitant assiste raisonnablement le Client dans le traitement :
• des demandes d'accès,
• des demandes de rectification,
• des demandes d'effacement,
• des demandes de limitation,
• des demandes de remise des données,
• des oppositions,
• d'autres prétentions en matière de protection des données.

Les frais supplémentaires peuvent être facturés selon le temps consacré si l'assistance n'est pas déjà comprise dans les prestations convenues.

16. Assistance concernant les obligations de protection des données

Le Sous-traitant assiste raisonnablement le Client concernant :
• les questions de sécurité des données,
• les violations de données personnelles,
• les analyses d'impact relatives à la protection des données,
• les informations techniques,
• les demandes des autorités de contrôle dans la mesure où elles concernent les Données traitées.

Les frais supplémentaires peuvent être facturés selon le temps consacré, dans la mesure autorisée par la loi et si l'assistance n'est pas déjà prévue au contrat.

17. Droits d'audit

Le Client peut vérifier, dans une mesure raisonnable, le respect du présent accord. Les Parties conviennent à l'avance du moment, de la durée, de l'étendue et des modalités de l'audit. Celui-ci peut être réalisé par un tiers externe indépendant et qualifié, soumis à une obligation de confidentialité.

L'audit ne doit pas perturber de manière disproportionnée l'exploitation du Sous-traitant. Les coûts sont à la charge du Client, sauf si l'audit révèle une violation contractuelle importante du Sous-traitant.

18. Restitution et suppression à la fin des relations contractuelles

À la fin des relations contractuelles qui fondent le présent accord, le Sous-traitant restitue ou supprime les Données traitées selon les instructions du Client, sauf si des obligations légales de conservation ou d'autres motifs juridiques s'y opposent.

La restitution s'effectue dans un format courant dans la mesure où elle est techniquement possible et contractuellement due.

Le Sous-traitant peut conserver des copies de sauvegarde pendant une période transitoire techniquement nécessaire, à condition qu'elles soient protégées de manière adéquate et supprimées à l'expiration de ce délai.

19. Utilisation de données anonymisées ou agrégées

Le Sous-traitant peut utiliser des données anonymisées ou agrégées aux fins suivantes :

- assurance qualité,
- amélioration du produit,
- analyses de sécurité,
- analyses statistiques,
- optimisation technique,
- justificatifs réglementaires,
- analyses scientifiques ou internes, dans la mesure où aucune réidentification n'est possible.

Une telle utilisation n'est autorisée que si elle ne permet pas de tirer des conclusions sur des patients individuels ou des informations confidentielles du Client.

20. Responsabilité

La responsabilité des Parties est régie par les dispositions applicables à la relation de base qui les lie.

21. Dispositions finales

Toute modification du présent accord doit être faite par écrit ou sous une forme électronique acceptée par les deux Parties.

Si certaines dispositions sont ou deviennent invalides, la validité des autres dispositions n'en est pas affectée.

Le droit suisse s'applique. Le for est Zurich.