

# Contrat de traitement des données personnelles

Accord entre le patient

– ci-après dénommé le « Patient » –

et

MyPhysio Swiss Sàrl

Route de Chancy 59C, 1213 Petit-Lancy, Suisse

CHE-483.719.272

– ci-après dénommé le « Fournisseur » –

relatif au traitement des données personnelles.

Préambule

Ce Contrat précise les obligations des parties relatives à la protection des données découlant de la relation entre le Patient et le Fournisseur. Elle s'applique à toutes les activités liées au contrat dans le cadre desquelles les données personnelles du Patient (ci-après dénommées « Données ») sont traitées par les employés du Fournisseur ou un sous-traitant mandaté par ce dernier.

## 1 Objet, durée et spécification du traitement des données personnelles

Les modalités relatives au service fourni par le Fournisseur sont détaillées dans le contrat conclu entre le Fournisseur et le Patient (ci-après dénommé « Contrat »).

(2) La durée de validité de ce Contrat est déterminée par la durée de relation entre le Patient et le Fournisseur, pour autant qu'aucune obligation supplémentaire ne découle des dispositions de ce Contrat.

## 2 Champ d'application et responsabilité

(1) Le Fournisseur traite les données décrites dans l'addendum A pour le compte du Patient aux fins et dans la mesure spécifiée dans celui-ci.

(2) Dans le cadre du présent Contrat, le Patient est seul responsable du respect des dispositions légales en matière de protection des données, et notamment de la légalité du transfert des données au Fournisseur ainsi que de la légalité du traitement des données.

(3) Les instructions sont initialement spécifiées dans le Contrat et peuvent être modifiées, complétées ou remplacées ultérieurement par le Patient au moyen d'instructions additionnelles, sous forme écrite ou électronique (sous forme textuelle), adressées au service désigné par le Fournisseur (instruction individuelle).

## 3 Obligations du Fournisseur

(1) Le Fournisseur ne peut traiter les données des personnes concernées que dans le cadre de la relation avec le Patient, sauf exceptions prévues par la loi.

(2) Dans son domaine de responsabilité, le Fournisseur adaptera l'organisation interne de l'entreprise de manière à répondre aux exigences spécifiques de la protection des données. Il prendra des mesures techniques et organisationnelles conformes aux exigences légales pour assurer la protection adéquate des données du Patient. Le Fournisseur doit prendre des mesures techniques et organisationnelles pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement des données sur une base permanente. Ces mesures techniques et organisationnelles sont connues du Patient, qui a la responsabilité de s'assurer qu'elles offrent un niveau de protection adéquat pour les risques des données à traiter.

(3) Les mesures prises par le Fournisseur sont décrites plus en détail dans l'addendum B. Les mesures techniques et organisationnelles font l'objet de progrès techniques et de développements ultérieurs. À cet égard, le Fournisseur est autorisé à mettre en œuvre d'autres mesures adéquates, à condition que le niveau de sécurité apporté par ces mesures ne soit pas être inférieur au niveau antérieur. Tout changement important doit être documenté.

(4) S'il en est ainsi convenu, le Fournisseur assiste le Patient dans la mesure de ses possibilités en cas de demande de renseignements et de réclamation des personnes concernées et dans le cadre du respect des obligations relatives à la protection des données.

(5) Le Fournisseur garantit que les employés et les autres personnes travaillant pour le Fournisseur impliqué dans le traitement des données du Patient ne sont pas autorisés à traiter les données en dehors de l'instruction. En outre, le Fournisseur garantit que les personnes autorisées à traiter les données personnelles sont liées par une obligation légale de confidentialité ou de secret professionnel. L'obligation de confidentialité ou de secret professionnel subsiste après l'exécution de la commande.

(6) Lorsqu'une violation de données à caractère personnel est constatée par le Fournisseur, il en informe immédiatement le Patient. Le Fournisseur prend les mesures nécessaires pour sécuriser les données et minimiser les éventuelles conséquences négatives pour les personnes concernées ; il en informe le Patient dans les plus brefs délais.

(7) Le Fournisseur met à la disposition du Patient l'interlocuteur suivant pour toute question relative à la protection des données dans le cadre du Contrat : le responsable de la protection des données de du Fournisseur, [secretariat@my-physio.ch](mailto:secretariat@my-physio.ch)

(8) Le Fournisseur s'engage à satisfaire ses obligations relatives à la protection des données, à établir une procédure en vue de contrôler périodiquement l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité du traitement.

Le Fournisseur corrige ou supprime les données faisant l'objet du contrat si le Patient le lui demande et que cela est compris dans le cadre de l'instruction. Si un effacement conforme à la protection des données ou une restriction correspondante du traitement des données ne s'avère pas possible, le Fournisseur procède à la destruction conforme à la protection des données des supports de données et autres matériels sur la base d'un mandat individuel par le Patient, ou restitue ces supports au Patient, à moins qu'il en ait été convenu autrement dans le Contrat.

Dans certains cas particuliers à déterminer par le Patient, un stockage, une remise, des mesures de compensation et de protection doivent être convenus séparément, à moins que le contrat ne les prévoie déjà.

(9) Les données, les supports de données ainsi que tous les autres documents doivent être remis ou supprimés après l'exécution de la commande sur demande du Patient. Si des coûts supplémentaires

résultent de spécifications divergentes dans le cadre de la communication ou de l'effacement des données, ces frais sont à la charge du Patient.

(10) Dans le cas d'une réclamation du Patient par une personne concernée portant sur le traitement des données, le Fournisseur s'engage à assister le Patient, dans la limite de ses possibilités, dans la défense de la réclamation en question.

(11) Les services correspondant aux points 3, 5, 6(2) et 6(3) (remise des supports de données, prise de contact avec les personnes concernées et vérifications, par exemple) doivent être remboursés au Fournisseur selon ses taux horaires actuels ou en fonction de ses dépenses externes.

## 4 Obligations du Patient

Le Patient s'engage à informer le Fournisseur en détail et dans les plus brefs délais s'il constate dans le site internet des erreurs ou des irrégularités concernant les dispositions relatives à la protection des données.

Le Patient donne autorisation à l'utilisation des ses données dans le respects des normes légales et du présent contrat

## 5 Demandes des personnes concernées

Si une personne concernée informe le Fournisseur de son souhait d'exercer son droit d'accès, de rectification ou d'effacement, le Fournisseur renverra cette personne au Patient, à condition qu'une mise en relation avec ce dernier soit possible en fonction des indications de la personne concernée. Le Fournisseur transmet immédiatement la demande de la personne concernée au Patient. Le Fournisseur assiste le Patient sur les instructions de ce dernier dans le cadre de ses possibilités et dans la mesure convenue. Le Fournisseur ne saurait être tenu responsable si la demande de la personne concernée ne fait l'objet d'aucune réponse ou fait l'objet d'une réponse inexacte ou tardive de la part du Patient.

## 6 Moyens de preuve

(1) Si, dans certains cas individuels, des inspections par le Patient ou un auditeur mandaté par ce dernier s'avèrent nécessaires, elles devront être effectuées pendant les heures de bureau normales sans occasionner de perturbation dans le fonctionnement de l'entreprise, après notification préalable et en tenant compte d'un délai raisonnable. Le Fournisseur peut les subordonner à une notification préalable avec un délai raisonnable et à la signature d'un accord de confidentialité portant sur les données des autres Patients et les mesures techniques et organisationnelles mises en place. Si l'auditeur mandaté par le Patient est en relation de concurrence avec le Fournisseur, le Fournisseur dispose contre celui-ci d'un droit d'opposition.

(2) Si une autorité de contrôle de la protection des données ou une autorité de contrôle publique de l'État membre du Patient procèdent à une inspection, le paragraphe 1 s'applique en conséquence. La signature d'un accord de confidentialité n'est pas requise si cette autorité de contrôle est soumise à une obligation légale de secret professionnel ou de confidentialité dont le non-respect est punissable conformément au Code pénal.

## 7 Obligations en matière d'information

(1) Si les données du Patient sont compromises en raison d'une saisie ou d'une confiscation, d'une procédure concordataire ou d'insolvabilité ou d'autres événements ou mesures de tiers, le Fournisseur doit informer le Patient dans les plus brefs délais. Le Fournisseur doit immédiatement informer toutes

les personnes responsables concernées de ce que la souveraineté et la propriété des données appartiennent exclusivement au Patient en tant que «responsable du traitement» au sens du règlement général sur la protection des données.

## 8 Responsabilité

(1) La responsabilité est régie par le Contrat.

## 9 Divers

(1) Les dispositions du Contrat s'appliquent par ailleurs. En cas de contradiction entre les dispositions de la présente Contrat et les dispositions du Contrat, la présente Contrat prévaut. Si telle ou telle disposition de la présente Contrat devait être nulle, la validité du Contrat et de l'Contrat n'en sera pas affectée.

(2) Les addenda A et B font partie intégrante de la présente Contrat.

## Addendum A de l'accord relatif au traitement des données personnelles

Objet du contrat:

Traitement des données personnelles du Patient dans le cadre de son utilisation du site internet

Nature et objectif du traitement prévu des données :

Les données personnelles du Patient sont transférées au Fournisseur pour les services de physiothérapie, ergothérapie ou similaires. Le Fournisseur traite ces données exclusivement en fonction de l'accord conclu.

Type des données personnelles :

Les types de données dépendent des données transmises par le Patient. Ce sont :

- Des données personnelles de base (nom, date de naissance, adresse, employeur), y compris des coordonnées (téléphone et e-mail, par exemple)
- Des données relatives au service, y compris les données relatives à la facturation et au paiement

Catégories de personnes concernées :

Effacement, blocage et rectification des données :

Toute demande d'effacement, de blocage et de rectification doit être adressée au Patient ; les dispositions du Contrat s'appliquent par ailleurs.

## Addendum B

Au contrat relatif au traitement des données de la commande

Mesures techniques et organisationnelles (MTO)

### 1 Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles (abrégées en MTO) suivantes sont indispensables pour le traitement des données

#### (1) Contrôle d'accès aux locaux et aux installations :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle d'accès :

- (i). Définition de zones de sécurité
- (ii). Mise en place d'une protection d'accès efficace
- (iii). Définition des personnes autorisées
- (iv). Gestion et documentation des autorisations d'accès du personnel sur l'ensemble du cycle de vie
- (v). Accompagnement des visiteurs et du personnel externe
- (vi). Surveillance des espaces en dehors des heures de fermeture
- (vii). Journalisation des accès physiques

#### (2) Contrôle d'accès aux systèmes :

- (i). Protection de l'accès (authentification)
- (ii). Authentification simple des collaborateurs (par nom d'utilisateur et mot de passe) avec un haut niveau de protection
- (iii). Blocage en cas d'échec d'authentification ou d'inactivité et processus de réinitialisation des identifiants d'accès bloqués
- (iv). Pas de fonction de mémorisation possible pour les mots de passe et/ou la saisie de formulaires
- (v). Définition des personnes autorisées
- (vi). Gestion et documentation des supports d'authentification du personnel et des autorisations d'accès
- (vii). Blocage d'accès automatique
- (viii). Blocage d'accès manuel
- (ix). Transmission sécurisée des identifiants d'authentification (credentials) dans le réseau
- (x). Journalisation des accès

#### (3) Contrôle d'accès aux données :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle d'accès aux données :

- (i). Elaboration d'un concept d'autorisation
- (ii). Mise en œuvre de restrictions d'accès
- (iii). Attribution d'autorisations minimales
- (iv). Gestion et documentation des autorisations d'accès aux données
- (v). Journalisation des accès aux données

#### (4) Contrôles des transports et des transferts :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des transferts

- (i). Transfert de données sécurisé entre le serveur et le Patient
- (ii). Sauvegarde de la transmission dans le back-end

- (iii). Sécurisation de la transmission vers des systèmes externes
- (iv). Implémentation de passerelles sécurisées au niveau des points de transmission du réseau
- (v). Renforcement des systèmes back-end
- (vi). Description de toutes les interfaces et des champs de données personnelles transmis
- (vii). Authentification machine-machine
- (viii). Gestion des disques (procédure)
- (ix). Procédure de collecte et d'élimination
- (x). Procédure de suppression/effacement respectueuse dans le respect de la protection des données

#### (5) Contrôle des saisies :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des saisies :

- (i). Documentation des autorisations de saisie
- (ii). Journalisation des saisies

#### (6) Contrôle des commandes :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des commandes :

- (i). Documentation des autorisations de saisie
- (ii). Journalisation des commandes

#### (7) Contrôle des disponibilités :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des disponibilités :

- 1) Concept de sauvegarde
- 2) Plan d'urgence
- 3) Stockage des sauvegardes
- 4) Contrôle des systèmes de secours

#### (8) Principe de séparation :

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des usages:

- 1) Modération dans la collecte des données
- 2) Traitement séparés