Accordo sul trattamento dei dati (ATD) mediduxTM

tra

[Nome del Cliente]
[Indirizzo]
[CAP, località]
Svizzera

di seguito il «Cliente»

e

mobile Health AG
Mühlebachstrasse 43
8008 Zurigo
Svizzera

di seguito il «Responsabile del trattamento»

congiuntamente le «Parti»

Indice

1. Scopo dell'accordo 3
2. Ruoli delle Parti 3
3. Oggetto, natura e finalità del trattamento 3
4. Categorie di dati personali 4
5. Categorie di interessati 5
6. Durata del trattamento 5
7. Istruzioni del Cliente 5
8. Obblighi del Cliente 5
9. Obblighi del Responsabile del trattamento 6
10. Riservatezza 6
11. Luogo del trattamento 6
12. Sub-responsabili 6
13. Misure tecniche e organizzative 7
14. Notifica delle violazioni dei dati personali 7
15. Assistenza per l'esercizio dei diritti degli interessati 7
16. Assistenza in relazione agli obblighi di protezione dei dati 8
17. Diritti di audit 8
18. Restituzione e cancellazione al termine dei rapporti contrattuali 8
19. Utilizzo di dati anonimizzati o aggregati 8
20. Responsabilità 9
21. Disposizioni finali 9

1. Scopo dell'accordo

Il presente Accordo sul trattamento dei dati disciplina i diritti e gli obblighi delle Parti in relazione al trattamento di dati personali da parte del Responsabile del trattamento per conto del Cliente nell'ambito dell'utilizzo di medidux™.

Integra l'offerta, le Condizioni generali / Condizioni d'uso di medidux™ SaaS e gli eventuali ulteriori accordi tra le Parti.

In caso di disposizioni divergenti rispetto ai documenti sopra indicati, prevale il presente Accordo.

2. Ruoli delle Parti

Nell'ambito dell'utilizzo di medidux™, il Cliente determina le finalità e i mezzi del trattamento dei dati dei pazienti e degli altri dati personali ed è pertanto titolare del trattamento ai sensi della normativa sulla protezione dei dati.

Il Responsabile del trattamento tratta i dati personali per conto e secondo le istruzioni del Cliente, salvo i casi eccezionali in cui adempie a propri obblighi legali o assume responsabilità proprie.

3. Oggetto, natura e finalità del trattamento

Il trattamento ha per oggetto la messa a disposizione tecnica, la conservazione, la trasmissione, la visualizzazione, il supporto, il backup e la valutazione dei dati nell'ambito dell'utilizzo concordato di medidux™.

Il trattamento viene effettuato in particolare per le seguenti finalità:

- messa a disposizione della piattaforma medidux™,
- raccolta strutturata di informazioni relative ai pazienti,
- visualizzazione di dati relativi a sintomi, parametri vitali, medicamenti, decorso, questionari, laboratorio e diagnostica,
- trattamento, visualizzazione, trasmissione e conservazione di dati di laboratorio e diagnostici se previsti nell'ambito dei servizi concordati, tramite inserimenti manuali, caricamenti o interfacce collegate,
- supporto alla comunicazione e all'assistenza da parte del Cliente,
- trattamento, visualizzazione, trasmissione e conservazione di dati di genomica, patologia molecolare, biomarcatori, moduli, registri, studi, board e consulti se previsti nell'ambito dei servizi concordati, tramite inserimenti manuali, caricamenti o interfacce collegate,
- amministrazione tecnica,
- assistenza,
- analisi degli errori,
- backup dei dati,
- messa a disposizione di report o esportazioni, se concordata,
- svolgimento dei processi di studio o assistenza concordati.

4. Categorie di dati personali

Il trattamento può comprendere in particolare le seguenti categorie di dati personali (di seguito anche «Dati trattati»):

- dati anagrafici dei pazienti,
- dati di contatto,
- data di nascita,
- sesso,
- numeri dei pazienti o identificativi interni,
- dati sanitari,
- diagnosi,
- sintomi,
- livelli di gravità,
- benessere,
- parametri vitali,
- peso,
- pressione sanguigna,
- polso,
- saturazione di ossigeno,
- temperatura,
- glicemia,
- dati ECG, se utilizzati,
- valori CRP, se utilizzati,
- dati di laboratorio e valori diagnostici se previsti nell'ambito dei servizi applicabili,
- referti e parametri di laboratorio, intervalli di riferimento, orari di prelievo, orari dei referti e relativi metadati trattati tramite interfacce, inserimenti manuali, caricamenti o sistemi collegati,
- dati di genomica, patologia molecolare e biomarcatori se previsti nell'ambito dei servizi applicabili,
- dati di moduli, moduli di inserimento strutturati, moduli di documentazione medica e relative informazioni di approvazione o stato,
- dati relativi a riunioni mediche interdisciplinari, consulti specialistici e board, comprese sintesi dei casi, domande, raccomandazioni, decisioni, verbali e relative informazioni mediche, se previsti nell'ambito dei servizi applicabili,
- dati di registri e studi, compresi dati relativi all'inclusione, all'evoluzione, ai risultati e alla documentazione dei registri, se previsti nell'ambito dei servizi applicabili,
- medicamenti,
- eventi terapeutici,
- effetti collaterali,
- risposte ai questionari,
- comunicazioni,
- note sul trattamento o sull'evoluzione,
- informazioni relative agli studi,
- stato di salute,
- dati tecnici di utilizzo,
- dati di log,
- dati relativi agli utenti e alle autorizzazioni.

Il trattamento concreto dei dati dipende dall'ambito dei servizi concordato tra le Parti, dalla configurazione del sistema e dalle eventuali interfacce concordate.

5. Categorie di interessati

Gli interessati possono comprendere in particolare:

- pazienti del Cliente,
- partecipanti agli studi,
- utenti del Cliente,
- professionisti sanitari,
- personale infermieristico,
- personale di studio,
- collaboratori amministrativi,
- amministratori tecnici.

6. Durata del trattamento

Il trattamento inizia con l'entrata in vigore del rapporto di base tra le Parti (cfr. punto 1) o con l'inizio dell'utilizzo di medidux™, a seconda dell'evento che si verifica per primo.

Il trattamento termina con la cessazione del rapporto di base, salvo che vi si oppongano obblighi legali di conservazione, interessi legittimi, istruzioni del Cliente o periodi di transizione tecnica.

7. Istruzioni del Cliente

Il Responsabile del trattamento tratta i Dati trattati esclusivamente secondo le istruzioni del Cliente, purché documentate per iscritto o in formato elettronico.

Costituiscono istruzioni in particolare:

- il presente Accordo,
- l'offerta / il modulo d'ordine e gli eventuali ulteriori documenti che disciplinano il rapporto di base tra le Parti,
- la configurazione concordata del sistema,
- le istruzioni del Cliente comunicate per iscritto o documentate elettronicamente.

Il Responsabile del trattamento informa il Cliente qualora ritenga che un'istruzione violi le disposizioni sulla protezione dei dati. Non sussiste un obbligo generale di effettuare una verifica legale completa.

8. Obblighi del Cliente

Il Cliente garantisce che:

- il trattamento dei dati è lecito,
- i pazienti vengono informati adeguatamente,
- vengono ottenuti i consensi necessari,
- è disponibile l'eventuale liberazione necessaria dal segreto medico,
- l'utilizzo di medidux™ è conforme alle direttive interne,
- l'accesso è concesso soltanto a persone autorizzate,
- le autorizzazioni sono assegnate e aggiornate correttamente,
- vengono rispettati i diritti degli interessati,
- vengono adempiuti gli obblighi di documentazione medica e legale.

Il Cliente è responsabile dell'esattezza, dell'ammissibilità e della liceità dei dati inseriti dal Cliente stesso, dai suoi utenti o dai pazienti.

9. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento si impegna a:

- trattare i Dati trattati soltanto per le finalità concordate,
- mantenere riservati i Dati trattati,
- concedere l'accesso soltanto alle persone che ne hanno bisogno per le proprie mansioni,
- imporre un obbligo di riservatezza alle persone che accedono ai Dati trattati,
- attuare misure tecniche e organizzative adeguate,
- assistere adeguatamente il Cliente nell'esercizio dei diritti degli interessati,
- segnalare tempestivamente le violazioni dei dati personali,
- ricorrere a sub-responsabili soltanto in conformità al presente Accordo,
- restituire o cancellare i Dati trattati alla fine del contratto secondo le istruzioni, salvo obblighi legali contrari.

10. Riservatezza

Il Responsabile del trattamento garantisce che tutte le persone che accedono ai Dati trattati siano soggette a un obbligo legale o contrattuale di riservatezza.

L'obbligo di riservatezza continua anche dopo la cessazione del rapporto contrattuale.

11. Luogo del trattamento

Salvo diverso accordo, i Dati trattati vengono conservati in Svizzera.

Il trattamento o l'accesso da Paesi che non offrono un livello adeguato di protezione dei dati è consentito soltanto se sono soddisfatte le condizioni richieste, in particolare mediante garanzie adeguate quali clausole contrattuali standard o misure equivalenti.

12. Sub-responsabili

Il Responsabile del trattamento può incaricare sub-responsabili se necessario per la fornitura dei servizi.

Il Responsabile del trattamento garantisce che i sub-responsabili siano vincolati contrattualmente agli obblighi di protezione e sicurezza dei dati e di riservatezza.

Il Cliente viene informato adeguatamente delle modifiche sostanziali relative ai sub-responsabili.
Se il Cliente si oppone a un nuovo sub-responsabile per un importante motivo relativo alla protezione dei dati entro un termine ragionevole, le Parti cercano una soluzione adeguata. Se non è possibile trovare una soluzione, il Cliente può disdire la parte di servizio interessata.

Il Responsabile del trattamento risponde dell'adempimento degli obblighi di protezione dei dati da parte dei sub-responsabili come del proprio comportamento.

13. Misure tecniche e organizzative

Il Responsabile del trattamento adotta misure tecniche e organizzative adeguate per proteggere i Dati trattati.

Tali misure riguardano in particolare:

- controllo degli accessi,
- controllo degli ingressi,
- gestione degli utenti e delle autorizzazioni,
- cifratura, ove adeguata,
- registrazione dei log,
- processi di backup e ripristino,
- protezione contro gli accessi non autorizzati,
- riservatezza,
- integrità,
- disponibilità,
- resilienza dei sistemi,
- processi per rilevare e gestire incidenti di sicurezza,
- trasmissione sicura dei dati,
- separazione dei dati, ove necessario,
- verifica e miglioramento periodici delle misure di sicurezza.

Il Responsabile del trattamento può adeguare le misure di sicurezza purché il livello di sicurezza non venga ridotto in modo sostanziale.

14. Notifica delle violazioni dei dati personali

Il Responsabile del trattamento informa il Cliente senza indugio non appena viene a conoscenza di una violazione della sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati, accidentali o illeciti ai Dati trattati.

Se disponibili, la notifica comprende:
• natura della violazione,
• categorie di dati interessate,
• categorie di persone interessate,
• numero approssimativo di persone interessate,
• possibili conseguenze,
• misure adottate o proposte,
• punto di contatto per eventuali domande.

Le informazioni non immediatamente disponibili possono essere fornite successivamente.

15. Assistenza per l'esercizio dei diritti degli interessati

Se un interessato contatta direttamente il Responsabile del trattamento per esercitare i propri diritti, quest'ultimo inoltra la richiesta al Cliente nella misura in cui riguarda i Dati trattati.

Il Responsabile del trattamento assiste adeguatamente il Cliente nell'elaborazione di:
• richieste di accesso,

• richieste di rettifica,
• richieste di cancellazione,
• richieste di limitazione,
• richieste di consegna dei dati,
• opposizioni,
• altre pretese in materia di protezione dei dati.

Gli oneri aggiuntivi possono essere fatturati in base al tempo impiegato se l'assistenza non è già inclusa nell'ambito dei servizi concordato.

16. Assistenza in relazione agli obblighi di protezione dei dati

Il Responsabile del trattamento assiste adeguatamente il Cliente in relazione a:
• questioni di sicurezza dei dati,
• violazioni dei dati personali,
• valutazioni d'impatto sulla protezione dei dati,
• informazioni tecniche,
• richieste delle autorità di controllo nella misura in cui riguardano i Dati trattati.

Gli oneri aggiuntivi possono essere fatturati in base al tempo impiegato, nei limiti consentiti dalla legge e se l'assistenza non è già prevista dal contratto.

17. Diritti di audit

Il Cliente ha il diritto di verificare in misura ragionevole il rispetto del presente Accordo. Le Parti concordano preventivamente il momento, la durata, l'ambito e le modalità dell'audit. L'audit può essere svolto da un soggetto esterno indipendente e qualificato, vincolato alla riservatezza.

L'audit non deve compromettere in modo sproporzionato l'attività del Responsabile del trattamento. I costi sono a carico del Cliente, salvo che l'audit accerti una violazione contrattuale sostanziale da parte del Responsabile del trattamento.

18. Restituzione e cancellazione al termine dei rapporti contrattuali

Al termine dei rapporti contrattuali su cui si basa il presente Accordo, il Responsabile del trattamento restituisce o cancella i Dati trattati secondo le istruzioni del Cliente, salvo che lo impediscano obblighi legali di conservazione o altri motivi giuridici.

La restituzione avviene in un formato corrente, se tecnicamente possibile e contrattualmente dovuto.

Il Responsabile del trattamento può conservare copie di backup per un periodo transitorio tecnicamente necessario, purché siano protette adeguatamente e cancellate alla scadenza di tale periodo.

19. Utilizzo di dati anonimizzati o aggregati

Il Responsabile del trattamento può utilizzare dati anonimizzati o aggregati per le seguenti finalità:
- garanzia della qualità,
- miglioramento del prodotto,
- analisi di sicurezza,

- analisi statistiche,
- ottimizzazione tecnica,
- documentazione per finalità normative,
- valutazioni scientifiche o interne, se non è possibile una re-identificazione.

Tale utilizzo è consentito soltanto se non è possibile risalire a singoli pazienti o a informazioni riservate del Cliente.

20. Responsabilità

La responsabilità delle Parti è disciplinata dalle disposizioni applicabili al rapporto di base tra le stesse.

21. Disposizioni finali

Le modifiche al presente Accordo devono essere effettuate per iscritto o in una forma elettronica accettata da entrambe le Parti.

L'eventuale invalidità di singole disposizioni non pregiudica la validità delle restanti disposizioni.

Si applica il diritto svizzero. Il foro competente è Zurigo.