

INFORMATIVA SULLA PRIVACY PER L'EUROPA

Benvenuti su myoncare, il portale digitale per la salute e l'app mobile ("**app**") per un'assistenza efficiente e on-demand ai pazienti e un supporto per i programmi di gestione della salute.

Per noi di Oncare GmbH (di seguito "**ONCARE**" oppure "**noi**", "**Noi**", "**nostro**"), la protezione della tua privacy e di tutti i dati personali che ti riguardano durante l'utilizzo dell' **app** è di grande importanza. Siamo consapevoli della responsabilità che deriva dalla tua fiducia nella fornitura e nell'archiviazione dei tuoi dati personali (sanitari) nell'app myoncare. Pertanto, i nostri sistemi tecnologici utilizzati per i servizi myoncare sono impostati secondo gli standard più elevati e il trattamento lecito dei dati è al centro della nostra comprensione etica come azienda.

Trattiamo i tuoi dati personali in conformità con la legislazione applicabile in materia di protezione dei dati personali, in particolare il Regolamento generale sulla protezione dei dati dell'UE ("**GDPR**") e le leggi specifiche del paese che si applicano a noi. La presente informativa sulla privacy spiega perché e come **ONCARE** elabora i tuoi dati personali (sanitari) che raccogliamo da te o che ci fornisci quando decidi di utilizzare l'app Myoncare. In particolare, troverete una descrizione dei dati personali che raccogliamo e trattiamo, nonché lo scopo e le basi su cui trattiamo i dati personali e i diritti che vi spettano.

Si prega di leggere attentamente l'Informativa sulla privacy per assicurarsi di aver compreso ogni disposizione. Dopo aver letto l'Informativa sulla privacy, l'utente ha la possibilità di accettare l'Informativa sulla privacy e di acconsentire al trattamento dei propri dati personali (sanitari) come descritto nell'Informativa sulla privacy. Se l'utente fornisce il proprio consenso, l'Informativa sulla privacy diventa parte del contratto tra l'utente e ONCARE.

Secondo le condizioni di utilizzo, la nostra offerta è rivolta solo a persone di età pari o superiore a 18 anni. Di conseguenza, non vengono memorizzati ed elaborati dati personali di bambini e adolescenti di età inferiore ai 18 anni.

In caso di questioni di interpretazione o controversie, solo la versione tedesca dell'informativa sulla privacy sarà vincolante e autorevole.

DEFINIZIONI

"**utente dell'app**" indica qualsiasi utente dell'App myoncare (Paziente e/o Dipendente).

"**Blockchain**" è un altro database decentralizzato nel sistema myoncare che memorizza i dati corrispondenti dell'applicazione.

"**società**" indica il datore di lavoro se l'utente e il suo datore di lavoro utilizzano gli strumenti myoncare per la gestione della salute sul lavoro del datore di lavoro.

"**Fornitore di servizi dati**" indica qualsiasi agente incaricato e istruito dalla Società per raccogliere, rivedere e interpretare i dati dei dipendenti pseudonimizzati o anonimizzati nei programmi di gestione della salute sul lavoro basati su un contratto di servizio separato con la Società (ad es. analista di dati, servizi generali di prevenzione sanitaria, servizi di valutazione dei dati, ecc.), che viene fornito da una scheda informativa separata ai dipendenti.

"**Medico**" indica il medico, la clinica, la struttura sanitaria o altro operatore sanitario che agisce da solo o per conto del medico, della clinica o della struttura sanitaria.

"**Percorso**" è un piano di trattamento standardizzato composto da diverse attività di cura programmate, che possono determinare le fasi per le diagnosi e le terapie.

"**Compiti di cura**" sono compiti o azioni specifiche all'interno di un percorso che devono essere svolte dagli operatori sanitari coinvolti, dal personale infermieristico o dal paziente stesso.

"**Applicazione myoncare**" indica l'applicazione mobile myoncare per l'utilizzo da parte di pazienti o dipendenti che desiderano utilizzare i servizi offerti da ONCARE.

"**Portale myoncare**" è il portale web myoncare, destinato all'uso professionale da parte degli utenti del portale e funge da interfaccia tra gli utenti del portale e gli utenti dell'app.

"**Strumenti MyonCare**" indica l'app myoncare e il portale myoncare insieme.

"**Applicazione myoncare PWA**" indica l'applicazione myoncare Progressive Web App per i pazienti che

desiderano utilizzare i servizi offerti da ONCARE tramite l'App PWA e non tramite l'App myoncare.

"**Servizi myoncare**" indica i servizi, le funzionalità e le altre offerte che sono o possono essere offerte agli utenti del portale tramite il Portale myoncare e/o agli utenti dell'app tramite l'app myoncare.

"**ONCARE**" significa ONCARE GmbH, Germania.

"**Utente del portale**" indica qualsiasi fornitore di servizi sanitari, società o fornitori di servizi dati che utilizza il portale myoncare basato sul web.

"**Informativa sulla privacy**" indica la presente dichiarazione fornita all'utente in qualità di paziente e utente dell'app myoncare, che descrive le modalità di raccolta, utilizzo e archiviazione delle informazioni personali dell'utente e informa l'utente dei suoi ampi diritti.

"**Condizioni d'uso**" indica i termini di utilizzo per l'utilizzo dell'App myoncare.

TRATTAMENTO DEI DATI

Oncare GmbH, una società registrata presso il Tribunale distrettuale di Monaco di Baviera con il numero di registrazione 219909 con sede legale in Balanstraße 71a, 81541 Monaco di Baviera, Germania, offre l'applicazione mobile **Applicazione myoncare** e la gestisce come l'accesso ai **Servizi MyonCare**. Questo **Informativa sulla privacy** si applica a tutti i dati personali trattati da ONCARE in relazione all'utilizzo dell' **Applicazione myoncare**.

CHE COSA SONO I DATI PERSONALI

"**dati personali**" indica qualsiasi informazione che consente di identificare una persona fisica. In particolare, ciò include il nome, la data di nascita, l'indirizzo, il numero di telefono, l'indirizzo e-mail e l'indirizzo IP.

"**dati sanitari**" indica i dati personali relativi alla salute fisica e mentale di una persona fisica, compresa la fornitura di servizi sanitari da cui precedono le informazioni sul suo stato di salute.

I dati sono da considerarsi "**anonimi**" se non è possibile stabilire un legame personale con la persona/utente.

Al contrario, "**dati pseudonomizzati**" sono dati da cui un riferimento personale o informazioni di identificazione personale sono sostituiti da uno o più identificatori artificiali o pseudonimi, ma che generalmente possono essere re identificati dalla chiave di identificazione.

Applicazione myoncare PWA

Una progressive web app (PWA) è un sito web che ha l'aspetto e le funzionalità di un'app mobile. Le PWA sono progettate per sfruttare le funzionalità native dei dispositivi mobili senza la necessità di un app store. L'obiettivo delle PWA è quello di combinare la differenza tra le app e il web tradizionale portando i vantaggi delle app mobili native nel browser. La PWA si basa sulla tecnologia di "React". "React" è un software open source per applicazioni PWA.

Per utilizzare l' **Applicazione myoncare PWA**, i pazienti hanno bisogno di un computer o di uno smartphone e di una connessione Internet attiva. Non è necessario scaricare un'app.

Alcuni dei servizi dell'app myoncare non possono essere utilizzati all'interno dell' **Applicazione myoncare PWA**, vedere la descrizione di seguito per i dettagli. I servizi o le specifiche sono i seguenti:

- Chatta con gli **operatori sanitari**;
- Video;
- Codici PIN di sicurezza;
- Tracciamento dei dati dell'attività (ad es. tramite AppleHealth, GoogleFit, Withings).

Le seguenti informazioni sull' **applicazione myoncare** si applicano anche all' **applicazione myoncare PWA**, se non diversamente descritto in questa sezione.

QUALI DATI PERSONALI VENGONO UTILIZZATI QUANDO SI UTILIZZA L'APP MYONCARE

Possiamo elaborare le seguenti categorie di dati su di te quando utilizzi l' **applicazione myoncare**:

Dati operativi: Dati personali che ci fornisci al momento della registrazione nella nostra **applicazione myoncare**, contattandoci in merito a problemi con l'app o interagendo in altro modo con noi allo scopo di utilizzare l'app.

Dati del trattamento: Tu o il tuo medico ci fornite i vostri dati personali, come nome, età, altezza, peso, indicazione, sintomi di malattia e altre informazioni relative al vostro trattamento (ad es. in un piano di cura). Le informazioni relative al trattamento includono, a titolo esemplificativo ma non esaustivo: informazioni sui farmaci assunti, risposte a questionari che includono informazioni relative a malattie o condizioni, diagnosi e terapie fornite dall' **operatore sanitario**, attività pianificate e completate.

Dati sull'attività: Dati personali che vengono elaborati da noi se si collega l' **applicazione myoncare** a un'applicazione sanitaria (ad es. GoogleFit, AppleHealth, Withings). I dati della tua attività saranno trasferiti al tuo affiliato **fornitori di servizi sanitari** come **utenti del portale**.

Dati di ricerca commerciali e non commerciali:

Trattiamo i tuoi dati personali in forma anonima/pseudonimizzata al fine di analizzare e produrre rapporti scientifici riassuntivi al fine di migliorare prodotti, trattamenti e risultati scientifici.

Dati sulla sicurezza del prodotto: Dati personali trattati per adempiere ai nostri obblighi legali in qualità di produttore del **Applicazione myoncare** come dispositivo medico. Inoltre, i dati personali dell'utente possono essere trattati da dispositivi medici o aziende farmaceutiche per adempiere a finalità di sicurezza legale o di vigilanza.

Dati di rimborso: Dati personali necessari per il processo di rimborso tra il tuo fornitore di servizi sanitari e il tuo fornitore di assicurazione sanitaria.

Dati sulla gestione della salute sul lavoro: Dati personali o aggregati raccolti in specifici progetti e questionari su richiesta del Suo **società** (direttamente o tramite un fornitore di servizi dati incaricato dalla vostra azienda). I dati possono riguardare determinate informazioni sulla salute, la tua opinione sul tuo benessere personale, la tua opinione come dipendente su una particolare situazione interna o esterna o dati sull'assistenza o la salute in generale.

TECNOLOGIA BLOCKCHAIN

Blockchain Tecnologia ("Blockchain") (brevetto europeo n. 4 002 787) è un servizio opzionale che non è obbligatorio. È il tuo **fornitore sanitario** che decide di utilizzare la soluzione blockchain. Le **Blockchain** si basa sulla tecnologia di Hyperledger Fabric. Hyperledger Fabric è un software open source per implementazioni blockchain a livello aziendale. Offre una piattaforma scalabile e sicura che supporta progetti di blockchain.

La blockchain nel sistema myoncare è un database aggiuntivo che memorizza i dati dell'applicazione. Tutti i dati della blockchain **sono** conservati nella Repubblica Federale di Germania. Si tratta di un privato **Blockchain ("Blockchain privata")**, consente solo l'input di partecipanti verificati selezionati ed è possibile sovrascrivere, modificare o eliminare le voci secondo necessità.

In generale, il **Blockchain** è costituito da dati digitali in una catena di pacchetti chiamati "blocchi" che memorizzano le transazioni corrispondenti. Il modo in cui questi blocchi sono collegati tra loro è cronologico. Il primo blocco che viene creato è chiamato blocco genesis, e ogni blocco aggiunto successivamente ha un hash crittografico relativo al blocco precedente, consentendo di risalire alle transazioni e alle modifiche delle informazioni al blocco genesis. Tutte le transazioni all'interno dei blocchi sono convalidate e verificate attraverso un meccanismo di consenso blockchain per garantire che ogni transazione sia invariata.

Ogni blocco contiene l'elenco delle transazioni, un timestamp, il proprio hash e l'hash del blocco precedente. Un hash è una funzione che converte i dati digitali in una catena alfanumerica. Se una persona non autorizzata tenta di modificare i dati di un singolo blocco, anche l'hash del blocco cambierebbe e il collegamento a quel blocco andrebbe perso. In questo caso, il blocco non può più essere sincronizzato con gli altri. Questo processo tecnico impedisce l'uso di persone non autorizzate dalla manipolazione dei contenuti della catena blockchain. Se tutti i nodi (nodi di rete) tentano di sincronizzare le proprie copie, viene rilevato che una copia è stata modificata e la rete ritiene che tale nodo sia difettoso.

Nostro **Blockchain** è un privato **Blockchain**. Un privato **Blockchain** è decentralizzato. Si tratta di un cosiddetto sistema di registro distribuito (sistema digitale per la

registrazione delle transazioni), che funziona come un database chiuso. A differenza del **Blockchain** pubblico, che non sono "autorizzati", i **Blockchain** privati sono "autorizzati" perché per diventare utente è necessaria l'autorizzazione. A differenza del **Blockchain** pubblico, che è accessibile al pubblico a tutti, l'accesso ai servizi privati **Blockchain** dipende dall'autorizzazione per diventare un utente. Questa struttura consente di sfruttare la sicurezza e l'immutabilità della tecnologia blockchain pur essendo conformi alla protezione dei dati e rispettando in particolare le normative del Regolamento generale sulla protezione dei dati (GDPR). I record blockchain privati possono essere modificati, alterati o eliminati; in questo contesto significa che il valore di riferimento dell'UUID (Universally Unique Identifier) nel database del **Medico** viene eliminato. Inoltre, l'hash viene reso anonimo nel database blockchain, con il risultato che questo processo complessivo è conforme al Regolamento generale sulla protezione dei dati e sono garantiti i diritti dell'interessato (diritto alla cancellazione "diritto all'oblio", art. 17 GDPR).

Tipologia di dati memorizzati ed elaborati nella blockchain:

- Istituzioni/Leistungserbinger UUID
 - Pazienti-UUID
 - UUID dell'asset
 - Hash dei dati delle attività di cura e degli asset.
- (UUID: Universal Unique Identifier).

I dati memorizzati nel **Blockchain** è pseudo-anonimizzato.

Il nostro **Blockchain** è progettato per garantire la privacy dei dati in termini di integrità dei dati, profilo del paziente, risorse e **Compiti di cura** e farmaci. Per comunicare con il **Blockchain**, l'utente deve registrare una serie di chiavi pubbliche-private. Per comunicare con la blockchain, l'utente ha bisogno di diverse chiavi pubbliche-private; Il processo di registrazione genera certificati che vengono memorizzati in un database separato del **Medico** e sul cellulare del paziente. Una copia di backup della chiave del paziente viene crittografata e memorizzata nel **Sanità provider**, a cui può accedere solo il paziente.

In sede di verifica del consenso alla protezione dei dati, nel caso in cui l'**Operatore sanitario** vuole comunicare con il paziente, il sistema verifica se il paziente ha dato il consenso all'informativa sulla privacy **del fornitore di servizi sanitari**. La **Blockchain** serve quindi a garantire l'integrità e la responsabilità della cartella per garantire che il paziente abbia accettato l'Informativa sulla privacy.

Quando un **Medico** carica una nuova versione di un'informativa sulla privacy, l'hash del file viene memorizzato sul **blockchain**, e dopo che il paziente ha accettato l'informativa sulla privacy, tale interazione viene memorizzata sul **Blockchain**. Ogni volta che comunica con il paziente, il **Blockchain** Risponde confrontando l'hash con un flag che indica se il consenso del paziente è ancora valido per l'attuale informativa sulla privacy.

L'integrità del profilo del paziente è garantita anche dalla blockchain nella sincronizzazione del paziente. L'**Operatore sanitario** rileva immediatamente se il profilo del paziente non è sincronizzato o corrisponde al profilo sul telefono cellulare confrontando l'hash del profilo del paziente nel **Blockchain**. In questo modo, l'**operatore sanitario** raggiunge sufficiente aggiornamento per quanto riguarda il profilo del paziente.

Portale myoncare:

Se l'**operatore sanitario** decide di utilizzare la soluzione blockchain, ONCARE implementa uno strumento aggiuntivo, chiamato "Adapter Service", che viene utilizzato per comunicare con la **Blockchain**. L'istanza blockchain è ospitata da ONCARE.

Applicazione myoncare:

I pazienti possono connettersi alla stessa istanza blockchain utilizzando lo strumento Phone Manager, anch'esso ospitato da ONCARE. Anche l'hosting di questo servizio si trova presso ONCARE.

Base giuridica del trattamento dei dati: Trattamento dei dati da parte di ONCARE per l'**operatore sanitario** è realizzato sulla base dell'art. 28 GDPR (Accordo sul trattamento dei dati).

ELABORAZIONE DATI OPERATIVI

Applicabile a tutti gli utenti dell'app

L'utente può fornirci alcune informazioni personali quando ci contatta per comprendere le funzionalità e l'utilizzo dell' **applicazione myoncare**, in caso di richiesta di assistenza o in caso di offerte di supporto da noi avviate (via telefono).

Personale di servizio

Per conto del titolare del trattamento dei dati (ad esempio, un operatore sanitario), ti offriamo assistenza nella compilazione di questionari tramite supporto telefonico (chiamate in uscita) per ottimizzare la tua assistenza digitale al paziente. Nel caso in cui l'utente scelga di non utilizzare questo servizio, è libero di rifiutare e opporsi all'assistenza telefonica.

In caso di richiesta di assistenza o di chiamata in uscita, i seguenti dati personali possono essere visualizzati anche dai dipendenti autorizzati ONCARE:

- I dati personali che hai fornito al tuo **Medico** tramite la nostra **app** (ad es. nome, data di nascita, immagine del profilo, dettagli di contatto).
- I dati sanitari che hai fornito al tuo **Medico, Fornitore di servizi dati o società** tramite la nostra **Applicazione myoncare** (ad es. informazioni sui farmaci assunti, risposte a questionari con informazioni relative a malattie o condizioni, diagnosi e terapie da parte di operatori sanitari, compiti pianificati e completati).

Dipendenti ONCARE autorizzati che possono accedere al database del tuo **operatore sanitario, fornitore di servizi dati o società** ai fini dell'elaborazione di una richiesta di servizio o dell'esecuzione di una chiamata in uscita, sono contrattualmente obbligati a mantenere tutti i dati personali strettamente riservati.

Notifiche push ed e-mail

Nell'ambito del supporto da parte di myoncare, desideriamo informarti su come gestiamo le notifiche e le informazioni importanti che ti inviamo.

1. Notifiche push:

- Ti inviamo notifiche push tramite il nostro **myoncare PWA** (Progressive Web App) e l' **Applicazione myoncare**

per informarti su attività, appuntamenti e aggiornamenti importanti.

- Hai la possibilità di disabilitare queste notifiche push nelle impostazioni della tua app.

2. Notifiche via e-mail:

- Indipendentemente dal fatto che tu abbia abilitato o disabilitato le notifiche push, continueremo a inviarti informazioni importanti e promemoria via e-mail.
- In questo modo ti assicuri di non perdere nessuna notifica importante e che il tuo supporto funzioni senza intoppi.

Perché lo facciamo:

- Il nostro obiettivo è quello di tenerti informato sulle tue attività e sugli aggiornamenti importanti per supportare al meglio la tua salute.
- Le e-mail sono un modo affidabile per garantire che le informazioni importanti ti raggiungano, anche quando le notifiche push sono disabilite.

Le tue opzioni di azione:

- Se non si desidera ricevere notifiche push, è possibile disattivarle nelle impostazioni dell' **Applicazione myoncare**.
- Assicurati che il tuo indirizzo e-mail sia accurato e aggiornato per garantire la corretta ricezione dei nostri messaggi.
- Se non si desidera ricevere promemoria via e-mail, è possibile disattivarli nelle impostazioni del **Applicazione myoncare**.

Periodo di archiviazione

I dati che ci fornisci per ricevere e-mail saranno conservati da noi fino a quando non ti disconnetti dai nostri servizi e saranno cancellati sia dai nostri server che dai server di Sendgrid dopo che ti disconnetti.

Quando l' **Applicazione myoncare** viene scaricata, le informazioni necessarie vengono trasmesse al fornitore dell'app store. Non abbiamo alcun controllo su questa raccolta di dati e non ne siamo responsabili. Trattiamo i dati personali che ci vengono forniti dal fornitore dell'app store nell'ambito del nostro rapporto

contrattuale allo scopo di sviluppare ulteriormente la nostra **App Myoncare** e servizi.

Nel trattamento dei dati operativi, ONCARE agisce in qualità di titolare del trattamento responsabile del trattamento lecito dei dati personali dell'utente.

Tipi di dati: nome, indirizzo e-mail, numero di telefono, data di nascita, data di registrazione, pseudo-chiavi generate dall'app; Token del dispositivo per identificare il dispositivo, il numero di pseudo-identificazione, l'indirizzo IP, il tipo e la versione del sistema operativo utilizzato dal dispositivo.

L'app utilizza l'API di Google Maps per utilizzare le informazioni geografiche. Quando si usa Google Maps, Google raccoglie, elabora e utilizza anche i dati sull'uso delle funzioni della mappa. Informazioni più dettagliate sull'ambito, la base giuridica e lo scopo del trattamento dei dati da parte di Google, nonché il periodo di conservazione, sono disponibili nell'Informativa sulla privacy di Google.

Finalità del trattamento dei dati operativi: Utilizziamo i dati operativi per mantenere le funzionalità dell'**applicazione myoncare** e per contattarti direttamente se necessario o se veniamo contattati da te (ad es. in caso di modifiche ai termini e alle condizioni, supporto necessario, problemi tecnici, assistenza nella compilazione di questionari, ecc.).

Giustificazione del trattamento: Il trattamento dei dati operativi è giustificato sulla base dell'art. 6 par. 1 lett. b GDPR per l'esecuzione del contratto stipulato con ONCARE ai fini dell'utilizzo del **Applicazione myoncare**.

GEOLOCALIZZAZIONE IP

Utilizziamo un'applicazione di geolocalizzazione per i nostri servizi. Utilizziamo ipapi (fornito da apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Vienna, Austria) e Geoapify (fornito da Keptago Ltd., N. Nikolaidi e T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Cipro) per identificare la posizione degli utenti pazienti. Lo utilizziamo per proteggere le nostre applicazioni e per verificare la posizione dell'utente paziente per garantire che l'uso dei nostri servizi sia

conforme. Non combiniamo le informazioni che raccogliamo con altre informazioni sull'utente che potrebbero identificarlo. I dati elaborati da apilayer includono l'indirizzo IP del paziente e altri dettagli sulla posizione. La base giuridica per l'utilizzo è l'art. 6 par. 1 lett. 6 par. 1 1 lett. f del GDPR. I dati saranno cancellati quando lo scopo associato per il quale sono stati raccolti non esisterà più e non vi sarà più un obbligo legale di conservazione. Per ulteriori informazioni sulla loro politica sulla privacy, visitare il sito <https://ipapi.com/privacy/> e

TRATTAMENTO DEI DATI

Applicabile agli utenti dell'app che utilizzano l'app con il proprio medico

Durante l'utilizzo dell'**applicazione myoncare** il tuo **operatore sanitario** può inserire i tuoi dati personali nel **portale myoncare** per iniziare **servizi MyonCare** (ad es. creare la cartella del paziente, fornire un compito individuale, promemoria per l'assunzione di farmaci, ecc.). Inoltre, tu e il tuo **operatore sanitario** potete caricare documenti e file sull'**Applicazione myoncare** e sul **Portale myoncare** e condividerli tra di voi. Il tuo **Operatore Sanitario** può caricare un'**Informativa sulla privacy** per tua informazione e definire altri requisiti di consenso per te come paziente per i quali deve essere dato il tuo consenso. I file sono archiviati in un database cloud in Germania. Il tuo **operatore sanitario** può consentire la condivisione di tali file con altri **utenti del portale** all'interno della sua istituzione o di altri **fornitori di servizi sanitari** al di fuori della sua istituzione (consulta l'**operatore sanitario**) per scopi medici. Gli altri utenti del portale non hanno accesso a questi file a meno che l'accesso non sia fornito dall'**operatore sanitario**. Inoltre, il tuo **operatore sanitario** può chiederci di assistervi telefonicamente nella compilazione di questionari (chiamate in uscita). Ciò avviene esclusivamente sotto la direzione del vostro **operatore sanitario** ed esclusivamente da dipendenti autorizzati ONCARE.

Utilizzeremo e tratteremo i tuoi dati in conformità con quanto stabilito nel presente documento **informativa sulla privacy**, così come ci dai il tuo consenso.

Trattiamo tali dati personali, compresi i dati sanitari dell'utente, in base a un accordo con e in conformità con le istruzioni del tuo **operatore sanitario** (accordo sul trattamento dei dati). Ai fini del presente accordo sul trattamento dei dati, l'operatore **sanitario** è responsabile del trattamento dei dati personali e dei dati sanitari dell'utente ai sensi delle leggi applicabili in materia di protezione dei dati in qualità di responsabile dei dati e ONCARE è il responsabile del trattamento di tali dati personali (sanitari). Ciò significa che ONCARE elabora i dati personali solo in conformità con le istruzioni dell'operatore **sanitario**. In caso di domande o dubbi sul trattamento dei propri dati personali o sanitari, è necessario contattare l'operatore **sanitario** in primo luogo.

Tipi di dati: nome, data di nascita, informazioni sul profilo, dettagli di contatto e anche dati sanitari, come sintomi, foto, informazioni sui farmaci assunti, risposte a questionari comprese informazioni relative a malattie o condizioni, diagnosi e terapie di operatori sanitari, attività pianificate e completate.

Finalità del trattamento dei dati: Trattiamo i vostri dati al fine di poter fornire i nostri **Servizi MyonCare** al tuo **operatore sanitario** e a te. I vostri dati sanitari, che inserite nella nostra **Applicazione myoncare**, verranno utilizzati dal tuo **operatore sanitario** per consigli e supporto per te. Trattiamo questi dati personali in base a un accordo e in conformità con le istruzioni del vostro **operatore sanitario**. La trasmissione di questi dati di trattamento è pseudonimizzata e crittografata. Per esercitare i propri diritti in qualità di interessato, si prega di contattare il proprio **Medico**.

Giustificazione del trattamento dei dati: i tuoi dati personali (trattamento) saranno trattati dal tuo **operatore sanitario** conformemente alle disposizioni del **GDPR** e tutte le altre normative applicabili in materia di protezione dei dati. Le basi giuridiche per il trattamento dei dati derivano in particolare dall'art. 9 par. 2 lett. h **GDPR** per i dati sanitari in quanto dati meritevoli di particolare protezione, nonché il consenso dell'utente ai sensi dell'art. 6 par. 1 lett. A e 9 par. 2 lett. a **GDPR**. Il trattamento dei dati da parte di ONCARE per il vostro **Medico** viene effettuato anche sulla base dell'art. 28 **GDPR** (accordo di elaborazione degli ordini).

Il tuo **operatore sanitario**, in qualità di responsabile del trattamento dei dati, è responsabile dell'ottenimento del consenso dell'utente. Anche se puoi usare l'applicazione **myoncare** senza tale consenso, la maggior parte delle funzioni non funzionerà più (ad esempio, la condivisione dei dati con il tuo **operatore sanitario**). Pertanto, il rifiuto o la revoca del consenso al trattamento dei dati comporta una grave limitazione delle funzionalità dei servizi pp e il tuo **operatore sanitario** non può più supportarti tramite l'applicazione **myoncare**.

TRATTAMENTO DEI DATI SULL'ATTIVITÀ

Soltanto applicabile se l'utente accetta e attiva il trasferimento dei dati dell'attività tramite gli strumenti MyonCare

Strumenti MyonCare offre la possibilità di collegare l'**applicazione myoncare** con alcune app per la salute (ad es. AppleHealth, GoogleFit, Withings) che utilizzi ("**App per la salute**"). Al fine di consentire il trattamento dei dati dell'attività, otterremo preventivamente il tuo consenso al trattamento. Se la connessione viene stabilita dopo che l'utente ha dato il suo consenso, i dati dell'attività raccolti dall'**App per la salute** sarà messo a disposizione del vostro **Operatore Sanitario** allo scopo di fornire ulteriori informazioni contestuali sulla tua attività. Si prega di notare che i dati dell'attività non sono convalidati da **strumenti MyonCare** e non deve essere utilizzato dal tuo **operatore sanitario** a fini diagnostici come base per il processo decisionale medico. Si prega inoltre di notare che i vostri **operatori sanitari** non sono obbligati a verificare i dati della tua attività e non sono tenuti a fornirti alcun feedback in merito ai dati della tua attività.

I dati dell'attività vengono condivisi con il tuo **operatore sanitario** affiliato ogni volta che l'**applicazione myoncare** è accessibile. Puoi revocare il tuo consenso alla condivisione dei dati dell'attività in qualsiasi momento nelle impostazioni del **Applicazione myoncare**. Si prega di notare che i dati della tua attività non saranno condivisi da questo momento in poi. I dati dell'attività che sono già stati condivisi non verranno eliminati dal **Portale myoncare** dei tuoi **operatori sanitari** affiliati.

Il trattamento dei dati relativi all'attività ricade sotto la responsabilità dell'utente.

Tipi di dati: Il tipo e l'entità dei dati trasferiti dipendono dalla vostra decisione e dalla disponibilità di questi dati all'interno dell'app **per la salute**. I dati possono includere, tra gli altri, peso, altezza, passi effettuati, calorie bruciate, ore di sonno, frequenza cardiaca e pressione sanguigna.

Finalità del trattamento dei dati relativi all'attività: I dati della tua attività saranno messi a disposizione del tuo **operatore sanitario** con cui l'utente è in contatto allo scopo di fornire ulteriori informazioni contestuali sulla sua attività.

Giustificazione del trattamento: Il trattamento dei dati relativi all'attività è sotto la responsabilità dell'utente.

TRATTAMENTO DEI DATI SULLA SICUREZZA DEL PRODOTTO

Applicabile agli utenti dell'app il cui operatore sanitario utilizza la variante per dispositivi medici degli strumenti myoncare

L' **applicazione myoncare** è classificato e commercializzato come dispositivo medico secondo le normative europee sui dispositivi medici. In qualità di produttore dell'app, dobbiamo rispettare determinati obblighi legali (ad es. monitoraggio della funzionalità dell'app, valutazione delle segnalazioni di incidenti che potrebbero essere correlate all'utilizzo dell'app, tracciamento degli utenti, ecc.). Inoltre, l' **applicazione myoncare** permette te e il tuo **operatore sanitario** per comunicare e raccogliere dati personali su determinati dispositivi medici o medicinali utilizzati nel trattamento. I fabbricanti di tali dispositivi medici o medicinali hanno anche obblighi legali in materia di sorveglianza del mercato (ad es. raccolta e valutazione delle segnalazioni di reazioni avverse).

ONCARE è il titolare del trattamento dei dati sulla sicurezza dei prodotti.

Tipi di dati: Segnalazioni di casi, dati personali forniti in una segnalazione di incidente e risultati della valutazione.

Trattamento dei dati sulla sicurezza dei prodotti: Conserviamo e valutiamo tutti i dati personali in

relazione ai nostri obblighi legali in qualità di produttori di un dispositivo medico e trasmettiamo questi dati personali (se possibile dopo la pseudonimizzazione) alle autorità competenti, agli organismi notificati o ad altri responsabili dei dati con obblighi di vigilanza. Inoltre, conserveremo e trasferiremo i dati personali in relazione a dispositivi medici e/o medicinali se riceviamo comunicazioni da parte del tuo **operatore sanitario**, da te in qualità di paziente o da terzi (ad es. i nostri distributori o importatori degli **strumenti myoncare** nel tuo paese) che devono essere segnalati al produttore del prodotto affinché il produttore possa rispettare i suoi obblighi legali in materia di sicurezza del prodotto.

Giustificazione del trattamento dei dati sulla sicurezza dei prodotti: La base giuridica per il trattamento dei dati personali per l'adempimento degli obblighi legali in qualità di produttore di dispositivi medici o medicinali è l'art. 6 par. 1 lett. c, art. 9 par. 2 lett. i GDPR in combinato disposto con gli obblighi di monitoraggio post-commercializzazione previsti dalla legge sui dispositivi medici e dalla direttiva sui dispositivi medici (disciplinata dal 26 maggio 2021 nel capitolo VII del nuovo regolamento sui dispositivi medici (UE) 2017/745) e/o dalla legge sui medicinali.

MODIFICHE ALL'INFORMATIVA SULLA PRIVACY

Applicabile agli utenti dell'app che utilizzano l'app con il proprio medico a scopo di rimborso

L' **Applicazione myoncare** supporta il tuo **Operatore Sanitario** nell'avviare procedure standard per il rimborso dei costi per i servizi sanitari forniti all'utente tramite l' **Applicazione myoncare**. Al fine di consentire la procedura di rimborso, l' **Applicazione myoncare** supporta la raccolta dei tuoi dati personali (sanitari) da parte dell' **operatore sanitario** per la trasmissione di questi dati all'unità di pagamento dell'utente (l'Associazione dei medici dell'assicurazione sanitaria obbligatoria e/o la compagnia di assicurazione sanitaria). Questo trattamento dei dati è solo un trasferimento iniziale di dati per il **Medico** per ottenere il rimborso dalla tua compagnia di assicurazione sanitaria. Il tipo e la quantità di dati personali trattati non differisce da altre routine di rimborso di **Operatori sanitari**. Il tuo **operatore sanitario** è il responsabile dei dati di rimborso. ONCARE agisce in qualità di responsabile del

trattamento dei dati sulla base dell'accordo con il tuo **operatore sanitario**.

Tipi di dati: nome, diagnosi, indicazioni, trattamento, durata del trattamento, altri dati necessari per la gestione del rimborso.

Trattamento dei dati di rimborso: il tuo **operatore sanitario** trasmette i dati di trattamento necessari per il rimborso al pagatore (l'ente di assicurazione sanitaria obbligatorio e/o la compagnia di assicurazione sanitaria) e il pagatore elabora i dati di rimborso al fine di fornire il rimborso al **Medico**.

Giustificazione del trattamento dei dati di rimborso: I dati di rimborso vengono elaborati sulla base dei §§ 295, 301 SGB V, art. P par. 2 lett. b GDPR. Il trattamento dei dati da parte di ONCARE per il vostro **operatore sanitario** viene effettuato anche in base all'art. 28 GDPR (accordo di elaborazione degli ordini).

TRATTAMENTO DEI DATI RELATIVI ALLA GESTIONE DELLA SALUTE IN AZIENDA

Applicabile agli utenti dell'app che utilizzano l'app con la gestione della salute in azienda

Durante l'uso dell' **applicazione myoncare** nell' **azienda** di gestione della salute sul lavoro, alcuni dati personali (sanitari) sono trasmessi in forma aggregata come dati per la gestione della salute sul lavoro alla **società** e ai **fornitori di servizi dati** commissionati dalla **società** (ad es. analisti di dati o società di ricerca). Né la **società** né alcun **fornitore di servizi dati** può assegnare tali dati alla tua identità. ONCARE raccomanda di non condividere alcun dato personale durante l'uso di **servizi MyonCare** nell'ambito della gestione della salute in azienda.

Ciò significa che ONCARE e tutti i **fornitori di servizi dati** tratterà i dati per la gestione della salute sul lavoro solo in conformità con le disposizioni **dell'azienda**. Trattiamo tali dati per la gestione della salute sul lavoro, compresi i vostri dati sanitari, sulla base di un accordo con la vostra **società** e/o un **fornitore di servizi dati** e in conformità con le loro istruzioni. Ai fini del presente accordo, la **società** o il **fornitore di servizi dati** è il responsabile del trattamento dei dati dell'utente per finalità di gestione della salute sul lavoro e ONCARE e qualsiasi **fornitore di**

servizi dati ingaggiato dalla **società**, se presenti, sono i responsabili del trattamento di tali dati. In caso di domande o dubbi sul trattamento dei dati per la gestione della salute sul lavoro, è necessario contattare la **società** in primo luogo.

Finalità del trattamento dei dati nella gestione della salute sul lavoro: Trattiamo i vostri dati per la gestione della salute in azienda al fine di poter offrire a voi e all'**azienda** i nostri **Servizi myoncare**. I dati di gestione della salute della vostra azienda, che inserite nella nostra **Applicazione myoncare**, sarà utilizzato dalla **società** (direttamente o tramite un **Fornitore di servizi dati**) nella gestione della salute sul lavoro. Trattiamo questi dati per la gestione della salute sul lavoro nell'ambito di un accordo e in conformità con le istruzioni della **società** e/o un **fornitore di servizi dati** per la gestione della salute sul lavoro. La trasmissione di questi dati per la gestione della salute sul lavoro è pseudonimizzata e crittografata. Per esercitare i propri diritti in qualità di interessato, si prega di contattare la **società**.

Giustificazione del trattamento dei dati relativi alla gestione della salute sul lavoro: I vostri dati di gestione della salute in azienda saranno trattati dalla **società** conformemente alle disposizioni **GDPR** e tutte le altre normative applicabili in materia di protezione dei dati. La base giuridica per il trattamento dei dati è in particolare il consenso dell'utente ai sensi dell'art. 6 par. 1 lett. a e l'art. 9 par. 2 lett. a GDPR o un'altra base giuridica applicabile alla **società**. Il trattamento dei dati da parte di ONCARE alla **società** (direttamente o tramite un **operatore sanitario** commissionato dalla vostra azienda) si basa anche sull'art. 28 GDPR (Accordo sul trattamento dei dati).

La **società** in qualità di titolare del trattamento, è responsabile dell'ottenimento del consenso dell'utente se richiesto dalle norme sulla protezione dei dati e del trattamento dei dati per finalità di gestione della salute sul lavoro in conformità con le leggi applicabili in materia di protezione dei dati.

QUALE TECNOLOGIA VIENE UTILIZZATA DALL'APP MYONCARE?

Servizio di posta elettronica

Utilizziamo Brevo (fornito da Sendinblue GmbH, con sede in Köpenicker Straße 126, 10179 Berlino) e Sendgrid (fornito da Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Questi servizi di posta elettronica possono essere utilizzati per organizzare l'invio di e-mail. Sendgrid viene utilizzato per inviare e-mail di conferma, conferme di transazioni ed e-mail con informazioni importanti relative alle richieste. I dati inseriti dall'utente per la ricezione delle e-mail vengono memorizzati sui server di Sendgrid. Quando inviamo e-mail per tuo conto tramite SendGrid, utilizziamo una connessione protetta SSL.

La comunicazione tramite posta elettronica viene utilizzata per le attività seguenti:

- Accedere all'applicazione web per la prima volta;
- Reimpostazione della password per l'applicazione web;
- Creare un account per la domanda del paziente;
- Reimpostare la password per l'applicazione del paziente;
- Generazione e invio di un report;
- Sostituisci le notifiche push con le e-mail per **PWA** (Progressive Web App) nei seguenti casi:
 - (i) se un piano di assistenza termina tra un'ora;
 - (ii) se il farmaco è stato assegnato;
 - (iii) se l'Informativa sulla privacy è stata aggiornata;
 - (iv) quando un appuntamento viene inviato a pazienti e medici, in particolare per il tipo di appuntamento "videochiamata";
 - v) Qualsiasi informazione relativa a un **compito di cura** o se un **Operatore sanitario** ha assegnato un **compito di cura**.

Brevo (Informativa sulla privacy):

Informativa sulla privacy - Protezione dei dati personali | Brevo

SendGrid (Informativa sulla privacy):

[SendGrid](#)

Matomo

Questo è uno strumento di analisi web open source. Matomo (fornito da InnoCraft Ltd., Nuova Zelanda) non trasmette dati a server al di fuori del controllo di ONCARE. Matomo è inizialmente disabilitato quando si utilizzano i nostri servizi. Il comportamento dell'utente verrà registrato in forma anonima solo dopo che questi

avrà acconsentito attivamente. Se disattivato, verrà memorizzato un "cookie persistente", se le impostazioni del browser lo consentono. Questo cookie segnala a Matomo che non si desidera che il browser venga registrato.

Le informazioni sull'utilizzo raccolte dal cookie vengono trasmesse ai nostri server e lì memorizzate in modo da poter analizzare il comportamento dell'utente.

Le informazioni generate dal cookie sull'utilizzo da parte dell'utente sono:

- Ruolo utente;
- Geolocalizzazione dell'utente;
- Utente-OS;
- Tempo in cui l'utente ha utilizzato il contenuto;
- Indirizzo IP;
- Siti visitati via web / **PWA** (per ulteriori informazioni, consultare la sezione relativa alle PWA nella presente Informativa sulla privacy);
- pulsanti su cui l'utente fa clic nel **portale myoncare**, l'**applicazione myoncare** e **myoncare PWA**.

Le informazioni generate dal cookie non saranno trasmesse a terzi.

È possibile rifiutare l'uso dei cookie selezionando le impostazioni appropriate nel browser. Tuttavia, tieni presente che in questo caso potresti non essere in grado di utilizzare tutte le funzionalità. Per ulteriori informazioni, consultare:

<https://matomo.org/privacy-policy/>.

La base giuridica per il trattamento dei dati personali degli utenti è l'art. 6 par. 1 frase 1 lett. a GDPR. Il trattamento dei dati personali degli utenti ci consente di analizzare il comportamento di utilizzo. Valutando i dati ottenuti, possiamo raccogliere informazioni sull'utilizzo dei singoli componenti dei nostri servizi. Questo ci aiuta a migliorare continuamente i nostri servizi e la loro usabilità.

Trattiamo e conserviamo i dati personali solo per il tempo necessario a soddisfare lo scopo previsto.

TRASFERIMENTO SICURO DEI DATI PERSONALI

Adottiamo misure di sicurezza tecniche e organizzative adeguate per proteggere in modo ottimale i dati personali da noi memorizzati contro la manipolazione

accidentale o intenzionale, la perdita, la distruzione o l'accesso da parte di persone non autorizzate. I livelli di sicurezza vengono continuamente verificati in collaborazione con esperti di sicurezza e adattati ai nuovi standard di sicurezza.

Lo scambio di dati da e verso l'app è crittografato. Utilizziamo TLS e SSL come protocolli di crittografia per il trasferimento sicuro dei dati. Anche lo scambio di dati è crittografato e viene effettuato con pseudo-chiavi.

TRASFERIMENTI DI DATI / DIVULGAZIONE A TERZI

Trasmetteremo i tuoi dati personali a terzi solo nell'ambito delle disposizioni di legge o sulla base del tuo consenso. In tutti gli altri casi, le informazioni non saranno divulgate a terzi, a meno che non siamo obbligati a farlo a causa di norme legali obbligatorie (divulgazione a organismi esterni, comprese le autorità di vigilanza o di polizia).

Qualsiasi trasmissione di dati personali viene crittografata durante la trasmissione.

INFORMAZIONI GENERALI SUL CONSENSO AL TRATTAMENTO DEI DATI

Il consenso dell'utente costituisce anche il consenso al trattamento dei dati ai sensi della legge sulla protezione dei dati. Prima di concedere il tuo consenso, ti informeremo sullo scopo del trattamento dei dati e sul tuo diritto di opposizione.

Se il consenso riguarda anche il trattamento di categorie particolari di dati personali, l'**applicazione myoncare** vi informerà espressamente di ciò nell'ambito della procedura di consenso.

Trattamento di categorie particolari di dati personali ai sensi dell'art. 9 par. 1 GDPR può avvenire solo se ciò è richiesto dalla legge e non vi è motivo di presumere che i tuoi legittimi interessi precludano il trattamento di questi dati personali o che tu abbia dato il tuo consenso al trattamento di questi dati personali ai sensi dell'art. 9 par. 2 del GDPR.

Per il trattamento dei dati per il quale è richiesto il consenso dell'utente (come spiegato nella presente **informativa sulla privacy**), il consenso sarà ottenuto

nell'ambito del processo di registrazione. Dopo l'avvenuta registrazione, i consensi possono essere gestiti nelle impostazioni dell'account dell'**applicazione myoncare**.

DESTINATARI DEI DATI / CATEGORIE DI DESTINATARI

Nella nostra organizzazione, ci assicuriamo che solo le persone siano autorizzate a trattare i dati personali necessari per adempiere ai loro obblighi contrattuali e legali. I tuoi dati personali e i dati sanitari che inserisci nella nostra **applicazione myoncare** saranno messi a disposizione per il tuo **operatore sanitario e/o azienda** direttamente o tramite un **fornitore di servizi dati** (a seconda del tipo di utilizzo degli **Strumenti myoncare**).

In alcuni casi, **altri fornitori di servizi** supportano i nostri reparti specializzati nell'adempimento dei loro compiti. I necessari accordi sulla protezione dei dati sono stati conclusi con tutti i **fornitori** che sono responsabili del trattamento dei dati personali. Questi **fornitori** sono Google (Google Firebase), fornitori di cloud storage e supporto ai fornitori di servizi.

Google Firebase è un "database NoSQL" che consente la sincronizzazione tra il tuo **portale MyonCare del fornitore di servizi sanitari** e l'**applicazione myoncare**. NoSQL definisce un meccanismo per l'archiviazione dei dati che non è solo modellato in relazioni tabulari, consentendo una scalabilità "orizzontale" più semplice rispetto ai sistemi di gestione di database tabulari/relazionali in un cluster di macchine.

A questo scopo, una pseudo-chiave dell'**applicazione myoncare** viene memorizzato in Google Firebase insieme al corrispondente **piano di cura**. Il trasferimento dei dati è pseudonimizzato per ONCARE e i suoi fornitori di servizi, il che significa che ONCARE e gli altri suoi fornitori di servizi non possono stabilire una relazione con l'utente in qualità di interessato. Ciò si ottiene crittografando i dati durante il trasferimento tra l'utente e il suo **fornitori di servizi sanitari o società** (direttamente o a qualsiasi **fornitore di servizi dati**) e utilizzando pseudo-chiavi invece di identificatori personali come il nome o l'indirizzo e-mail per tracciare questi trasferimenti. La re identificazione avviene non appena i dati personali hanno raggiunto l'account del tuo **fornitori di servizi sanitari o società nel portale myoncare** o il tuo account nella sezione **applicazione myoncare**, dopo che è stato verificato da token specifici.

I nostri fornitori di cloud storage offrono spazio cloud in cui il Firebase manager, che gestisce gli URL Firebase per il **portale myoncare**, viene memorizzato. Inoltre, questi fornitori di servizi forniscono il dominio server isolato del **Portale myoncare**, in cui sono memorizzati i dati personali dell'utente. Ospita anche i servizi di gestione video e file di myoncare, che consentono videoconferenze crittografate tra l'utente e il suo **operatore sanitario** così come lo scambio di file. Accesso ai tuoi dati personali da parte tua e del tuo **operatore sanitario** è garantito dall'invio di token specifici. Questi dati personali sono crittografati durante il trasferimento e a riposo e pseudonimizzati per ONCARE e i suoi fornitori di servizi. I fornitori di servizi ONCARE non hanno mai accesso a questi dati personali.

Inoltre, ci avvaliamo di fornitori di servizi per elaborare le richieste di servizio (fornitori di servizi di supporto) relative all'utilizzo dell'account, ad esempio se hai dimenticato la password, desideri modificare il tuo indirizzo e-mail memorizzato, ecc. Con questi fornitori di servizi sono stati stipulati i necessari accordi per l'elaborazione degli ordini; Inoltre, i dipendenti incaricati dell'elaborazione delle richieste di servizio sono stati formati di conseguenza. Al ricevimento della richiesta di servizio, le verrà assegnato un numero di biglietto.

Se si tratta di una richiesta di servizio relativa all'utilizzo dell'account, le informazioni pertinenti che ci hai fornito quando ci hai contattato saranno inoltrate a uno dei dipendenti autorizzati del servizio esterno. Ti contatteranno quindi.

In caso contrario, continueranno ad essere trattati da personale ONCARE appositamente autorizzato come descritto nella sezione "TRATTAMENTO DEI DATI OPERATIVI".

Attraverso i nostri fornitori di servizi di supporto, utilizziamo lo strumento RepairCode, noto anche come Digital Twin Code, che è una piattaforma di customer experience per la gestione di feedback esterni con la possibilità di creare ticket di supporto. Qui puoi trovare l'informativa sulla privacy:

<https://app.repaircode.de/?main=main-client> –
[Legale/privacy](#).

Infine, mostriamo contenuti da Instagram (fornitore: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublino 2, Irlanda), come

immagini, video o post. Se fai clic su un post di Instagram collegato, verrai reindirizzato a Instagram. Durante questo processo, Instagram può impostare cookie ed elaborare i dati dell'utente.

Quando visiti una pagina contenente un post di Instagram collegato, il tuo browser potrebbe stabilire automaticamente una connessione ai server di Instagram. In questo modo Instagram riceve l'informazione che l'utente ha visitato il nostro sito web, anche se non dispone di un account Instagram o non ha effettuato l'accesso. Se hai effettuato l'accesso, Instagram potrebbe associare la visita al tuo account utente.

Informativa sulla privacy:

<https://privacycenter.instagram.com/policy>

TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI

Per fornire i nostri servizi, possiamo avvalerci di fornitori di servizi situati al di fuori dell'Unione Europea (paese terzo). Se i dati vengono trasferiti in un paese terzo in cui il livello di protezione dei dati personali è ritenuto inadeguato, ci assicuriamo che vengano adottate misure adeguate in conformità con il diritto nazionale ed europeo. Se necessario, ciò include l'attuazione di clausole contrattuali standard tra le parti del trattamento.

I dati personali raccolti dall'**applicazione myoncare** non sono memorizzati negli app store. I dati personali saranno trasferiti in paesi terzi (al di fuori dell'Unione Europea o dello Spazio Economico Europeo) solo se ciò è necessario per l'adempimento dell'obbligo contrattuale, è richiesto dalla legge o se l'utente ci ha fornito il suo consenso.

La sincronizzazione del **Applicazione myoncare** E la **Portale myoncare** avviene tramite Google Firebase. Il server di Google Firebase è ospitato nell'Unione Europea. Tuttavia, come descritto nei Termini di utilizzo di Google Firebase, sono possibili trasferimenti di dati a breve termine verso i paesi in cui si trovano Google o i suoi fornitori di servizi; per alcuni servizi di Google Firebase, i dati vengono trasferiti solo negli Stati Uniti, a meno che l'elaborazione non avvenga nell'Unione Europea o nello Spazio economico europeo. L'accesso illegale ai tuoi dati è impedito con la crittografia end-to-end e i token di accesso sicuri. I nostri server sono

ospitati in Germania. A scopo di analisi, le e-mail inviate con SendGrid contengono un cosiddetto "pixel di tracciamento" che si connette ai server di Sendgrid quando l'e-mail viene aperta. Questa funzione può essere utilizzata per determinare se un messaggio di posta elettronica è stato aperto.

Integriamo i contenuti di Instagram, forniti da Meta Platforms Ireland Ltd. Se si fa clic su un post di Instagram collegato, è possibile che i dati personali (ad es. indirizzo IP, informazioni sul browser, interazioni) vengano trasmessi a Meta Platforms Inc. negli Stati Uniti o in altri paesi terzi.

Meta è certificata ai sensi dell'accordo UE-USA Data Privacy Framework (DPF), che riconosce un livello adeguato di protezione dei dati per i trasferimenti negli Stati Uniti. Tuttavia, i dati possono essere trasferiti anche in paesi per i quali non esiste una decisione di adeguatezza da parte della Commissione europea. In tali casi, possono essere necessarie ulteriori misure di protezione, sebbene la loro efficacia non possa sempre essere pienamente garantita.

Base giuridica

Il trattamento dei dati si basa sul consenso dell'utente (art. 6 par. 1 lett. un GDPR). Puoi revocare il consenso in qualsiasi momento. La revoca rimane inalterata dalla liceità delle operazioni di trattamento dei dati già avvenute.

Si prega di notare che i dati dell'utente vengono solitamente trasmessi da noi a un server di SendGrid negli Stati Uniti e lì memorizzati. Abbiamo stipulato un contratto con Sendgrid che contiene le clausole contrattuali standard dell'UE. Ciò garantisce un livello di protezione paragonabile a quello dell'UE.

Per elaborare i dati delle attività, all'interno del sito vengono utilizzate interfacce con i servizi Google Cloud (nel caso di GoogleFit) o con AppleHealth o Withings **utente dell'app**. **Strumenti MyonCare** utilizza queste interfacce, fornite da Google, Apple e Withings, per richiedere dati sull'attività dalle app per la salute connesse. La richiesta inviata da **Strumenti MyonCare** non contiene dati personali. I dati personali sono messi a disposizione degli **strumenti dimyoncare** tramite queste interfacce.

DURATA DELLA CONSERVAZIONE DEI DATI PERSONALI

Conserviamo i tuoi dati personali per tutto il tempo necessario allo scopo per il quale sono stati trattati. Si prega di notare che numerosi periodi di conservazione richiedono la conservazione continua dei dati personali. Ciò vale in particolare, ma non solo, per gli obblighi di ritenzione previsti dal diritto commerciale o fiscale (ad es. codice commerciale, legge fiscale, ecc.). Inoltre, il tuo **Medico** deve inoltre garantire la conservazione delle cartelle cliniche (tra 1 e 30 anni, a seconda del tipo di documenti).

Si prega di notare che ONCARE è inoltre soggetta a obblighi di conservazione concordati contrattualmente con l' **operatore sanitario** in base alle disposizioni di legge. Inoltre, e solo se il tuo **operatore sanitario** utilizza la variante del dispositivo medico degli **strumenti Myoncare**, si applicano determinati periodi di conservazione derivanti dalla legge sui dispositivi medici a causa della classificazione dell' **applicazione myoncare** come dispositivo medico. Se non vi sono altri obblighi di conservazione, i dati personali saranno regolarmente cancellati non appena lo scopo è stato raggiunto.

Inoltre, possiamo conservare i dati personali se l'utente ci ha dato il suo consenso a farlo o se sorge un contenzioso e utilizziamo le prove entro i termini di prescrizione previsti dalla legge, che possono arrivare fino a 30 anni; Il termine di prescrizione regolare è di tre anni.

OBBLIGO DI FORNIRE I DATI PERSONALI

Diversi dati personali sono necessari per l'instaurazione, l'esecuzione e la cessazione del rapporto contrattuale e l'adempimento dei relativi obblighi contrattuali e di legge. Lo stesso vale per l'uso della nostra **Applicazione myoncare** e le varie funzioni che offre.

Abbiamo riassunto i dettagli per te nei punti precedenti. In alcuni casi, i dati personali devono essere raccolti o resi disponibili anche in conformità con le disposizioni di legge. Si prega di notare che senza fornire questi dati personali, non è possibile elaborare la richiesta o adempiere all'obbligo contrattuale sottostante.

ACCESSO

Per tutti i dispositivi, indipendentemente dal sistema operativo utilizzato, è necessario concedere all'app

determinate autorizzazioni, che chiamiamo "diritti di accesso di base". A seconda del sistema operativo del dispositivo che stai utilizzando, potrebbe avere funzionalità aggiuntive che richiedono autorizzazioni aggiuntive per il funzionamento dell'app. Affinché l'**Applicazione myoncare** funzioni sul tuo dispositivo, l'app deve ricevere varie autorizzazioni per accedere a determinate funzioni del dispositivo. Se applicabile, li elencheremo in ordine di sistema operativo (Android o iOS) in base alle "condizioni di base".

I diritti di accesso di base (Android e iOS) sono:

Ottieni connessioni Wi-Fi

Necessario per garantire la funzionalità del download dei documenti in combinazione con le connessioni Wi-Fi.

Ottieni connessione di rete

Necessario per garantire la funzionalità del download dei documenti in combinazione con connessioni di rete che non sono connessioni Wi-Fi.

Disattiva il blocco schermo (impedisce la modalità stand-by)

Necessario affinché i video che appartengono ai documenti forniti possano essere riprodotti direttamente nell'app senza essere interrotti da un blocco schermo.

Accesso a tutte le reti

L'accesso a tutte le reti è necessario per scaricare i documenti.

Disattiva la modalità di sospensione

Ciò è necessario affinché i video che appartengono ai documenti forniti possano essere riprodotti direttamente nell'app senza che la riproduzione venga interrotta dal verificarsi dell'ibernazione.

Dati mobili / Accesso ai dati mobili

Se l'utente desidera scaricare i documenti esclusivamente tramite Wi-Fi, può effettuare l'impostazione appropriata nel menu dell'app e disattivare l'uso dei dati mobili. L'accesso ai dati mobili è necessario per garantire la funzionalità di disabilitazione dei download di documenti sui dati mobili.

Accesso alla fotocamera

L'accesso alla fotocamera è necessario per la scansione dei codici QR e per le consultazioni video

Accesso al microfono

Per le consultazioni video è necessario l'accesso al microfono

Accedere a file e foto

Ciò è necessario per lo scambio di file tra l'utente e gli utenti del portale collegati.

Accesso tramite browser Web

Questa operazione è necessaria per visualizzare i file ricevuti dagli utenti del portale connessi.

Utilizziamo le notifiche push, che sono messaggi che vengono inviati al tuo dispositivo mobile come servizio dell'**applicazione myoncare** tramite servizi come Apple Push Notification Service o Google Cloud Messaging Service. Questi servizi sono funzionalità standard dei dispositivi mobili. L'Informativa sulla privacy del Fornitore di servizi disciplina l'accesso, l'uso e la divulgazione delle informazioni personali a seguito dell'utilizzo di questi servizi da parte dell'utente.

DECISIONI AUTOMATIZZATE NEI SINGOLI CASI

Per prendere decisioni utilizziamo un'elaborazione totalmente automatizzata.

I TUOI DIRITTI IN QUALITÀ DI INTERESSATO

Desideriamo informarvi sui vostri diritti in qualità di interessati. Tali diritti sono stabiliti negli articoli da 15 a 22 del GDPR e comprendono:

Diritto di accesso (art. 15 GDPR): L'utente ha il diritto di richiedere informazioni sull'eventuale trattamento dei propri dati personali e sulle modalità di trattamento dei propri dati, comprese le informazioni sulle finalità del trattamento, i destinatari, il periodo di conservazione, nonché i diritti di rettifica, cancellazione e opposizione. L'utente ha inoltre il diritto di ricevere una copia di tutti i dati personali in nostro possesso.

Diritto alla cancellazione / diritto all'oblio (Art. 17 GDPR): L'utente può chiederci di cancellare i propri dati personali raccolti e trattati da noi senza ingiustificato ritardo. In questo caso, ti chiederemo di eliminare l'**applicazione myoncare** compreso il tuo UID (numero di identificazione univoco) dal tuo smartphone/telefono cellulare. Si prega di notare, tuttavia, che possiamo cancellare i dati personali dell'utente solo dopo la

scadenza dei periodi di conservazione previsti dalla legge.

Diritto di rettifica (art. 16 GDPR): L'utente può chiederci di aggiornare o correggere i dati personali inesatti o di completare i dati personali incompleti.

Diritto alla portabilità dei dati (art. 20 GDPR): In linea di principio, l'utente può richiedere la fornitura di dati personali che ci ha fornito e che vengono elaborati automaticamente sulla base del suo consenso o dell'esecuzione di un contratto con l'utente in forma leggibile da una macchina, in modo che possano essere "trasferiti" a un fornitore di servizi sostitutivo.

Diritto alla limitazione del trattamento dei dati (Art. 18 GDPR): L'utente ha il diritto di richiedere la limitazione del trattamento dei propri dati personali se l'esattezza dei dati è contestata, se il trattamento è illecito, se i dati sono necessari per rivendicazioni legali o se è in corso un'obiezione al trattamento.

Diritto di opposizione al trattamento dei dati (art. 21 GDPR): L'utente ha il diritto di opporsi all'utilizzo dei propri dati personali da parte nostra e di revocare il proprio consenso in qualsiasi momento se trattiamo i suoi dati personali sulla base del suo consenso. Continueremo a fornire i nostri servizi se non dipendono dalla revoca del consenso.

Per esercitare tali diritti, si prega di contattare il proprio **Medico** o **società** in primo luogo o contattarci all'indirizzo: privacy@myoncare.com. L'opposizione e la revoca del consenso devono essere dichiarate in forma scritta a privacy@myoncare.com.

Ti chiederemo di fornire una prova sufficiente della tua identità per garantire che i tuoi diritti siano protetti e che i tuoi dati personali saranno divulgati solo a te e non a terzi.

Vi preghiamo di contattarci in qualsiasi momento all'indirizzo privacy@myoncare.com. Se avete domande sul trattamento dei dati nella nostra azienda o se desiderate revocare il vostro consenso. L'utente ha inoltre il diritto di contattare l'autorità di controllo competente per la protezione dei dati.

GARANTE DELLA PROTEZIONE DEI DATI

Per rispondere a tutte le domande sulla protezione dei dati, potete contattare il nostro responsabile della protezione dei dati all'indirizzo privacy@myoncare.com.

LIMITE DI ETÀ DELLA DOMANDA

È necessaria un'età minima di 18 anni per utilizzare l'App myoncare.

MODIFICHE ALL'INFORMATIVA SULLA PRIVACY

Ci riserviamo espressamente il diritto di modificare la presente **Informativa sulla privacy** in futuro a nostra esclusiva discrezione. Modifiche o aggiunte possono essere necessarie, ad esempio, per soddisfare i requisiti giuridici, per conformarsi agli sviluppi tecnici ed economici o per soddisfare gli interessi di **app** o **Utenti del portale**.

Le modifiche sono possibili in qualsiasi momento e saranno comunicate all'utente in modo appropriato e in un lasso di tempo ragionevole prima che diventino effettive (ad esempio, pubblicando un'informativa sulla privacy rivista al momento dell'accesso o fornendo un preavviso di modifiche sostanziali).

In caso di questioni di interpretazione o controversie, solo la versione tedesca dell'informativa sulla privacy sarà vincolante e autorevole.

ONCARE GmbH

Indirizzo postale

Balanstraße 71a

81541 Monaco di Baviera, Germania

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Informazioni di contatto del responsabile della protezione dei dati
privacy@myoncare.com

Ultimo aggiornamento il 20 febbraio 2025.

* * * *

Stati Uniti INFORMATIVA SULLA PRIVACY

Benvenuti su myoncare, il portale digitale per la salute e l'app mobile ("**App**") per un'assistenza efficiente e on-demand ai pazienti e un supporto per i programmi di gestione della salute sul lavoro.

La presente Informativa sulla privacy descrive le modalità di utilizzo e condivisione delle informazioni personali e mediche dell'utente e le modalità di accesso a tali informazioni. Si prega di leggere attentamente la presente Informativa sulla privacy. Nella presente informativa sulla privacy, scoprirai perché e come ONCARE elabora i tuoi dati sanitari personali forniti se decidi di utilizzare l'app myoncare.

Per noi di Oncare GmbH (di seguito denominati "**Oncare (ONCARE** oppure "**noi**", "**noi**", "**nostro**"), la protezione della tua privacy e dei dati personali che ti riguardano durante l'utilizzo dell'app myoncare è di grande rilevanza e importanza. Siamo consapevoli della responsabilità che deriva dalla tua fiducia nel fornire e archiviare i tuoi dati personali (sanitari) nell'app myoncare. Pertanto, i nostri sistemi tecnologici utilizzati per i servizi myoncare sono impostati secondo gli standard più elevati e il trattamento lecito dei dati è al centro della nostra comprensione etica come azienda.

Qualsiasi informazione in nostro possesso che viene fornita dall' **operatore sanitario** è considerata **Informazione sanitaria protetta (PHI)** e/o altre informazioni mediche. Questi sono protetti da alcune leggi, come gli Stati Uniti. Legge sulla portabilità e la responsabilità dell'assicurazione sanitaria (**HIPAA**). Abbiamo l'obbligo legale di proteggere la privacy e la sicurezza delle informazioni sanitarie protette. Ci sforziamo costantemente di proteggere le informazioni sanitarie attraverso mezzi amministrativi, fisici e tecnici e di rispettare le leggi federali e statali applicabili.

L'uso e la divulgazione di tali **PHI** è conforme alle politiche sulla privacy applicabili e Leggi. Per capire più in dettaglio come elaborarli e condividerli **PHI**, dovresti leggere questo **Informativa sulla privacy** attentamente. Si prega di leggere attentamente l'Informativa sulla privacy per assicurarsi di aver compreso ogni disposizione. Dopo aver letto l'Informativa sulla privacy, l'utente ha la possibilità di accettare l'Informativa sulla privacy e di acconsentire al trattamento dei propri dati

personali (sanitari) come descritto nell'Informativa sulla privacy. Se l'utente fornisce il proprio consenso, l'Informativa sulla privacy diventa parte del contratto tra l'utente e ONCARE. Garantiamo i diritti e gli obblighi descritti nella presente Informativa sulla privacy. Utilizziamo ed elaboriamo i vostri dati in conformità con le disposizioni della presente informativa sulla privacy.

Secondo le condizioni di utilizzo, la nostra offerta è rivolta solo a persone di età pari o superiore a 18 anni. Di conseguenza, non vengono memorizzati ed elaborati dati personali di bambini e adolescenti di età inferiore ai 18 anni.

DEFINIZIONI

"Utente dell'app" indica qualsiasi utente dell'App myoncare (Paziente e/o Dipendente).

"La tecnologia blockchain" Il sistema myoncare contiene un database aggiuntivo in cui sono memorizzati i dati di tutte le installazioni.

"società" indica il datore di lavoro se l'utente e il suo datore di lavoro utilizzano gli strumenti myoncare per la gestione della salute sul lavoro del datore di lavoro.

"Ente coperto" indica un piano sanitario, un centro di smistamento sanitario o un fornitore di servizi sanitari che invia informazioni sanitarie in formato elettronico in relazione a una transazione che rientra nell'HIPAA.

"Fornitore di servizi dati" indica qualsiasi agente incaricato e istruito dalla Società per raccogliere, rivedere e interpretare i dati dei dipendenti pseudonimizzati o anonimizzati nei programmi di gestione della salute sul lavoro sulla base di un accordo di servizio separato con la Società (ad esempio, analista di dati, servizi di prevenzione sanitaria generale, servizi di valutazione dei dati, ecc.), che viene fornito da una scheda informativa separata ai dipendenti.

"Regolamento generale sulla protezione dei dati dell'UE". Il Regolamento generale sulla protezione dei dati (GDPR) è una legge europea sulla protezione dei dati. Il regolamento è entrato in vigore il 25 maggio 2018 e mira ad armonizzare la protezione dei dati in tutti gli Stati membri e a dare ai cittadini un maggiore controllo sui propri dati personali. Il GDPR si applica a tutte le

aziende e organizzazioni che operano nell'UE o trattano dati personali di cittadini dell'UE, indipendentemente dal fatto che l'azienda si trovi all'interno o all'esterno dell'UE. Il GDPR si applica anche a te in qualità di cittadino statunitense perché Oncare ha sede in Germania.

"Operatore sanitario" indica il medico, la clinica, la struttura sanitaria o altro operatore sanitario che agisce da solo o per conto del medico, della clinica o della struttura sanitaria.

"Percorso" è un piano di trattamento standardizzato in grado di determinare i passaggi per le diagnosi e le terapie. **"Compiti di cura"** sono compiti o azioni specifiche all'interno di un percorso che devono essere svolte dagli operatori sanitari coinvolti, dal personale infermieristico o dal paziente stesso.

"Informazioni sanitarie" indica tutte le informazioni, comprese le informazioni genetiche, registrate oralmente o in qualsiasi forma o su qualsiasi supporto, e che

- elaborati o trasferiti da un fornitore di assistenza sanitaria, un piano sanitario, un'autorità sanitaria, un datore di lavoro, un assicuratore sulla vita, una scuola o un'università o un centro di scambio sanitario; e
- si riferisce alla salute fisica o mentale passata, presente o futura di una persona o a qualsiasi condizione di salute in relazione al trattamento medico della persona, a seconda dei casi;

- la remunerazione passata, presente o futura per l'assistenza sanitaria di una persona. **"Informazioni sanitarie protette"** oppure **"PHI"** indica informazioni sanitarie identificabili individualmente che

- (i) è trasmesso tramite mezzi elettronici;
- ii) sono conservati su supporti elettronici; o
- (iii) trasmessi o conservati in qualsiasi altra forma o mezzo.

"Legge sulla portabilità e la responsabilità dell'assicurazione sanitaria", The Health Insurance Portability and Accountability Act del 1996 (**HIPAA**) è un U.S. Legge federale che prevede la creazione di standard nazionali per proteggere le informazioni sanitarie sensibili dei pazienti dalla divulgazione non autorizzata senza il loro consenso o conoscenza. I requisiti HIPAA si applicano all'uso e alla divulgazione di informazioni

sanitarie di individui da parte di istituzioni soggette alla legge HIPAA. Questi individui e organizzazioni sono indicati come "entità coperte".

"Applicazione PWA myoncare" indica l'applicazione myoncare Progressive Web App per i pazienti che desiderano utilizzare i servizi offerti da ONCARE tramite l'App PWA e non tramite l'App myoncare.

"Portale myoncare" è il portale web myoncare, destinato all'uso professionale da parte degli utenti del portale e funge da interfaccia tra gli utenti del portale e gli utenti dell'app.

"Servizi MyonCare" indica i servizi, le funzionalità e le altre offerte che sono o possono essere offerte agli Utenti del Portale tramite il portale myoncare e/o agli Utenti dell'app tramite l'app myoncare.

"Strumenti MyonCare" indica l'app myoncare e il portale myoncare insieme.

"ONCARE" oppure **"noi"** indica ONCARE GmbH, con sede in Germania.

"Utente del portale" indica qualsiasi fornitore di servizi sanitari, aziende o fornitori di servizi dati che utilizzano il portale myoncare basato sul web.

"Informativa sulla privacy" indica la presente dichiarazione fornita all'utente in qualità di paziente o dipendente e utente dell'app myoncare, che descrive le modalità di raccolta, utilizzo e archiviazione dei dati personali dell'utente e lo informa dei suoi diritti.

"Applicazione myoncare" indica l'app mobile myoncare per l'utilizzo da parte di pazienti o dipendenti che desiderano utilizzare i servizi offerti da ONCARE.

"Condizioni d'uso" indica i termini di utilizzo per l'utilizzo dell'App myoncare.

CONFORMITÀ ALLE LEGGI

Oncare GmbH, una società registrata presso il Tribunale distrettuale di Monaco di Baviera con il numero di registrazione 219909 con sede legale in Balanstraße 71a, 81541 Monaco di Baviera, Germania, offre l'applicazione mobile **applicazione myoncare** e la gestisce come

l'accesso ai **servizi Myoncare**. La presente informativa sulla privacy si applica a tutti i dati personali trattati da ONCARE in relazione all'utilizzo dell' **applicazione myoncare**.

ONCARE è un "socio in affari" ai sensi dell'art. **HIPAA** che fornisce servizi e piani sanitari a **Fornitori di servizi sanitari** denominati "enti contemplati" ai sensi dell'art. **HIPAA**; ONCARE stipula accordi di partnership commerciali con queste società coperte. ONCARE elaborerà e condividerà solo il **PHI** ai sensi degli accordi e ai sensi dell' **HIPAA**.

Siamo richiesti dall'U.S. Noi siamo tenuti, in base alla legge statunitense, a mantenere la privacy e la sicurezza delle informazioni sanitarie protette dell'utente. Siamo obbligati dagli Stati Uniti Legge per seguire le leggi progettate per proteggere la privacy e la sicurezza delle informazioni sanitarie protette. Ti informeremo immediatamente se si verifica una violazione (la cosiddetta violazione dei dati) che potrebbe aver messo in pericolo la privacy o la sicurezza delle informazioni (sanitarie).

Dobbiamo rispettare gli obblighi e i contenuti descritti nella presente Informativa sulla privacy e fornirti una copia dell'Informativa sulla privacy su richiesta.

Nessuna informazione personale (sanitaria) identificabile sarà venduta.

Non utilizzeremo o condivideremo le informazioni dell'utente in modo diverso da quanto descritto qui, a meno che l'utente non ci dica che siamo autorizzati a farlo.

Stati Uniti Informativa sulla privacy, Stati Uniti Le leggi federali e statali possono imporre ulteriori restrizioni alla condivisione delle informazioni sanitarie in relazione a trattamenti medici per abuso di droghe o alcol, malattie sessualmente trasmissibili, informazioni genetiche o programmi di trattamento della salute mentale. Se si applicano le leggi pertinenti, otterremo il consenso dell'utente prima di condividere o elaborare questi dati.

COSA SONO I DATI PERSONALI AI SENSI DEL GDPR

Trattiamo i dati personali dell'utente in conformità con le disposizioni di legge applicabili in materia di protezione dei dati personali, in particolare il Regolamento generale sulla protezione dei dati dell'UE e le leggi specifiche del paese che ci riguardano. Troverai una descrizione dei dati personali che raccogliamo e trattiamo, nonché lo scopo e la base su cui trattiamo i dati personali e i diritti a cui hai diritto.

"**Dati personali**" indica qualsiasi informazione che consente di identificare una persona fisica. In particolare, ciò include il nome, la data di nascita, l'indirizzo, il numero di telefono, l'indirizzo e-mail e l'indirizzo IP.

"**Dati sanitari**" indica i dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la fornitura di servizi sanitari che rivelano informazioni sul suo stato di salute.

I dati sono considerati "**anonimi**" se non è possibile stabilire un riferimento personale alla persona/utente. Al contrario, dati "**pseudonimizzati**" sono dati in cui il riferimento personale o i dati personali sono sostituiti da uno o più identificatori artificiali o pseudonimi, ma che generalmente possono essere re identificati con la chiave identificativa (ai sensi dell'art. 4 n. 5 GDPR).

myoncare PWA-App

Una progressive web app (PWA) è un sito web che ha l'aspetto e le funzionalità di un'app mobile. Le PWA sono progettate per sfruttare le funzionalità native dei dispositivi mobili senza la necessità di un app store. L'obiettivo delle PWA è quello di combinare la differenza tra le app e il web tradizionale portando i vantaggi delle app mobili native nel browser. La PWA si basa sulla tecnologia di "React". "React" è un software open source per applicazioni PWA.

Per utilizzare il **myoncare PWA**, i pazienti hanno bisogno di un computer o di uno smartphone e di una connessione Internet attiva. Non è necessario scaricare un'app.

Alcuni dei servizi dell' **applicazione myoncare** non possono essere utilizzati nell'ambito di **myoncare PWA**, vedere la descrizione di seguito per i dettagli. I servizi o le specifiche sono i seguenti:

- Chatta con **Fornitori di servizi sanitari**;
- Video;
- Codici PIN di sicurezza;
- Tracciamento dei dati dell'attività (ad es. tramite AppleHealth, GoogleFit, Withings).

Le seguenti informazioni sull' **applicazione myoncare** si applicano anche a **myoncare PWA**, se non diversamente descritto in questa sezione

QUALI DATI PERSONALI VENGONO UTILIZZATI QUANDO SI UTILIZZA L'APP MYONCARE

Utilizziamo e condividiamo le informazioni sanitarie dell'utente per le normali attività commerciali che rientrano nelle categorie di trattamento e assistenza sanitaria previste dalla legge. Possiamo elaborare le seguenti categorie di dati su di te quando utilizzi l'**applicazione myoncare**:

Dati operativi: Dati personali che ci fornisci al momento della registrazione nella nostra **applicazione myoncare**, contattandoci in caso di problemi con l'app o interagendo in altro modo con noi allo scopo di utilizzare l'app.

Dati del trattamento: Lei o il suo medico inserite dati personali come nome, età, altezza, peso, indicazione, sintomi di malattia e altre informazioni in relazione al vostro trattamento (ad es. in un piano di cura) con il supporto del **Applicazione myoncare**. Le informazioni relative al trattamento includono, a titolo esemplificativo ma non esaustivo: informazioni sui farmaci assunti, risposte a questionari che includono informazioni relative a malattie o condizioni, diagnosi e terapie fornite dall' **operatore sanitario** , attività pianificate e completate).

Dati sull'attività: Dati personali che vengono elaborati da noi se si collega il **Applicazione myoncare** a un'app per la salute (ad es. GoogleFit, AppleHealth, Withings). I dati della tua attività saranno trasferiti al tuo **operatore sanitario** come utenti del portale.

Dati di ricerca commerciali e non commerciali: Trattiamo i tuoi dati personali in forma anonima/pseudonimizzata al fine di analizzare e

produrre rapporti scientifici riassuntivi al fine di migliorare prodotti, trattamenti e risultati scientifici.

Dati sulla sicurezza del prodotto: Dati personali trattati per adempiere ai nostri obblighi legali in qualità di produttore del **Applicazione myoncare** come dispositivo medico. Inoltre, i dati personali dell'utente possono essere trattati da aziende di dispositivi medici o farmaceutiche per soddisfare obiettivi di sicurezza legale o di vigilanza.

Informazioni sul rimborso: Dati personali necessari per il processo di rimborso tra il tuo **Operatore sanitario** di myoncare e la tua compagnia di assicurazione sanitaria.

Dati sulla gestione della salute sul lavoro: dati personali o aggregati raccolti in specifici progetti e questionari su richiesta della **società** (direttamente o tramite un **fornitore di servizi dati** a contratto dalla **società**). I dati possono riguardare determinate informazioni sulla salute, la tua opinione sul tuo benessere personale, la tua opinione come dipendente su una particolare situazione interna o esterna o dati sull'assistenza o la salute in generale.

TECNOLOGIA BLOCKCHAIN

Blockchain **Tecnologia ("Blockchain")** (brevetto europeo n. 4 002 787) è un servizio opzionale che non è obbligatorio. Spetta al tuo **operatore sanitario**, decidere di utilizzare la soluzione blockchain. Le **Blockchain** si basa sulla tecnologia di Hyperledger Fabric. Hyperledger Fabric è un software open source per implementazioni blockchain a livello aziendale. Offre una piattaforma scalabile e sicura che supporta i progetti blockchain.

La **Blockchain** nel sistema myoncare è un database aggiuntivo che memorizza i dati dell'applicazione. Tutti i dati blockchain sono archiviati nella Repubblica Federale Tedesca. Si tratta di una **Blockchain** privata ("**Blockchain privata**"), consente solo l'input di partecipanti verificati selezionati ed è possibile sovrascrivere, modificare o eliminare le voci secondo necessità.

In generale, la **Blockchain** è costituito da dati digitali in una catena di pacchetti chiamati "blocchi" che memorizzano le transazioni corrispondenti. Il modo in cui questi blocchi sono collegati tra loro è cronologico. Il primo blocco che viene creato è chiamato blocco genesi, e ogni blocco aggiunto successivamente ha un hash

crittografico relativo al blocco precedente, consentendo di risalire alle transazioni e alle modifiche delle informazioni al blocco genesi. Tutte le transazioni all'interno dei blocchi sono convalidate e verificate attraverso un meccanismo di consenso blockchain per garantire che ogni transazione sia invariata.

Ogni blocco contiene l'elenco delle transazioni, un timestamp, il proprio hash e l'hash del blocco precedente. Un hash è una funzione che converte i dati digitali in una catena alfanumerica. In questo caso, il blocco non può più essere sincronizzato con gli altri. Se una persona non autorizzata tenta di modificare i dati di un singolo blocco, anche l'hash del blocco cambierebbe e il collegamento a quel blocco andrebbe perso. Se tutti i nodi (nodi di rete) tentano di sincronizzare le proprie copie, viene rilevato che una copia è stata modificata e la rete ritiene che tale nodo sia difettoso. Questo processo tecnico impedisce a persone non autorizzate di **manipolare** il contenuto della catena blockchain.

La nostra **Blockchain** è una **Blockchain privata**. Una **Blockchain privata** è decentralizzata. Si tratta di un cosiddetto sistema di registro distribuito (sistema digitale per la registrazione delle transazioni), che funziona come un database chiuso. A differenza delle **Blockchain** pubbliche, che sono "non autorizzate", le **Blockchain** private sono "autorizzate" perché per diventare utente è necessaria l'autorizzazione. A differenza delle **Blockchain** pubbliche, che sono accessibili al pubblico a tutti, l'accesso ai servizi privati **Blockchain** dipende dall'autorizzazione per diventare un utente. Questa struttura permette di sfruttare la sicurezza e l'immutabilità di **Tecnologia blockchain** nel rispetto della protezione dei dati, e in particolare per rispettare le disposizioni del regolamento generale sulla protezione dei dati (**GDPR**). I record blockchain privati possono essere modificati, alterati o eliminati; in questo contesto significa che il valore di riferimento dell'UUID (Universally Unique Identifier) nella banca dati dell'**operatore sanitario** viene eliminato. Inoltre, l'hash viene reso anonimo nel database blockchain, con il risultato che questo processo complessivo è conforme al Regolamento generale sulla protezione dei dati e sono garantiti i diritti dell'interessato (diritto alla cancellazione "diritto all'oblio", art. 17 GDPR).

Tipologia di dati memorizzati ed elaborati nella blockchain:

- Pazienti-UUID
- Istituzioni/Leistungserbinger UUID
- UUID dell'asset
- Hash di **compito di cura** e dati sulle risorse.
(UUID: *identificatore univoco universale*).

I dati memorizzati nel **Blockchain** è pseudo-anonimizzato.

Nostro **Blockchain** è progettato per garantire la privacy dei dati in termini di integrità dei dati, profilo del paziente, risorse e **Compiti di cura** e farmaci. Per comunicare con il **Blockchain**, l'utente deve registrare una serie di chiavi pubbliche-private. Per comunicare con la **Blockchain**, l'utente ha bisogno di diverse chiavi pubbliche-private; Il processo di registrazione genera certificati che vengono memorizzati in un database separato dell'**operatore sanitario** e sul cellulare del paziente. Una copia di backup della chiave del paziente viene crittografata e memorizzata nel database dell'**operatore sanitario**, a cui può accedere solo il paziente.

In sede di verifica del consenso alla protezione dei dati, nel caso in cui l'**operatore sanitario** desidera comunicare con il paziente, il sistema verifica se il paziente ha dato il consenso all'Informativa sulla privacy del Fornitore. La **Blockchain** serve quindi a garantire l'integrità e la responsabilità della cartella per garantire che il paziente abbia accettato l'Informativa sulla privacy.

Quando un **operatore sanitario** carica una nuova versione di un'informativa sulla privacy, l'hash del file viene memorizzato sulla **Blockchain**, e dopo che il paziente ha accettato l'informativa sulla privacy, tale interazione viene memorizzata sulla **Blockchain**. Ogni volta che comunica con il paziente, la **Blockchain** risponde confrontando l'hash con un flag che indica se il consenso del paziente è ancora valido per l'attuale informativa sulla privacy.

L'integrità del profilo del paziente è garantita anche dalla blockchain nella sincronizzazione del paziente. L'**operatore sanitario** riconosce immediatamente se il profilo del paziente non si sincronizza o non corrisponde al profilo sul telefono cellulare confrontando l'hash del profilo del paziente nella **Blockchain**. In questo modo, l'**operatore sanitario** raggiunge aggiornamento sufficiente per quanto riguarda il profilo del paziente.

Portale myoncare:

Se l' **operatore sanitario** decide di utilizzare la soluzione blockchain, ONCARE implementa uno strumento aggiuntivo, chiamato "Adapter Service", che viene utilizzato per comunicare con la **blockchain**. L'istanza blockchain è ospitata da ONCARE.

Applicazione myoncare:

I pazienti possono connettersi alla stessa istanza blockchain utilizzando lo strumento Phone Manager, anch'esso ospitato da ONCARE. Anche questo servizio è ospitato da ONCARE.

Giustificazione del trattamento: Il trattamento dei dati da parte di ONCARE per conto dell' **operatore sanitario** viene effettuato sulla base dell'art. 28 GDPR (accordo di elaborazione degli ordini).

ELABORAZIONE DATI OPERATIVI

Applicabile a tutti gli utenti dell'app

L'utente può fornirci alcune informazioni personali quando ci contatta per comprendere o discutere le funzionalità e l'utilizzo dell'app, in caso di richiesta di servizio o nel caso di offerte di supporto avviate da noi (via telefono).

Personale di servizio

Per conto del titolare del trattamento dei dati (ad esempio, un operatore sanitario), ti offriamo assistenza nella compilazione di questionari tramite supporto telefonico (chiamate in uscita) per ottimizzare la tua assistenza digitale al paziente. Nel caso in cui si scelga di non utilizzare questo servizio, si è liberi di rifiutare e opporsi all'assistenza telefonica.

In caso di richiesta di assistenza o di chiamata in uscita, i seguenti dati personali possono essere visualizzati anche dai dipendenti autorizzati ONCARE:

- i dati personali che hai fornito al tuo **operatore sanitario** tramite la nostra app (ad es. nome, data di nascita, immagine del profilo, dati di contatto);
- le informazioni sanitarie che hai fornito al tuo **operatore sanitario** al **Fornitore di servizi dati** o all'azienda tramite la nostra **applicazione myoncare** (ad es. informazioni sui farmaci assunti, risposte a questionari che includono informazioni relative a

malattie o condizioni, diagnosi e terapie da parte di operatori sanitari, compiti pianificati e completati).

Dipendenti ONCARE autorizzati che possono accedere al database del tuo **operatore sanitario, fornitori di servizi di dati o società** ai fini dell'elaborazione di una richiesta di servizio, sono contrattualmente obbligati a mantenere tutti i dati personali strettamente riservati.

Spiegazioni importanti sulle notifiche push e sulle e-mail

Nell'ambito del supporto da parte di myoncare, desideriamo informarti su come gestiamo le notifiche e le informazioni importanti che ti inviamo.

1. Notifiche push:

- Ti inviamo notifiche push tramite la nostra **myoncare PWA** (Progressive Webapp) e l' **applicazione myoncare** per informarti su attività, appuntamenti e aggiornamenti importanti.
- Hai la possibilità di disabilitare queste notifiche push nelle impostazioni della tua app.

2. Notifiche via e-mail:

- Indipendentemente dal fatto che tu abbia abilitato o disabilitato le notifiche push, continueremo a inviarti informazioni importanti e promemoria via e-mail.
- In questo modo ti assicuri di non perdere nessuna notifica importante e che il tuo supporto funzioni senza intoppi.

Perché lo facciamo:

- Il nostro obiettivo è quello di tenerti informato sulle tue attività e sugli aggiornamenti importanti per supportare al meglio la tua salute.
- Le e-mail sono un modo affidabile per garantire che le informazioni importanti ti raggiungano, anche quando le notifiche push sono disabilitate.

Le tue opzioni di azione:

- Se non si desidera ricevere notifiche push, è possibile disattivarle nelle impostazioni dell' **applicazione myoncare**.

- Assicurati che il tuo indirizzo e-mail sia accurato e aggiornato per garantire la corretta ricezione dei nostri messaggi.
- Se non si desidera ricevere promemoria via e-mail, è possibile disattivarli nelle impostazioni dell'Applicazione myoncare.

Periodo di archiviazione

I dati che ci fornisci per ricevere e-mail saranno conservati da noi fino a quando non ti disconnetti dai nostri servizi e saranno cancellati sia dai nostri server che dai server di Sendgrid dopo che ti disconnetti.

Quando l'applicazione myoncare vengono scaricate, le informazioni necessarie vengono trasmesse al fornitore dell'app store. Non abbiamo alcun controllo su questa raccolta di dati e non ne siamo responsabili. Trattiamo i dati personali che ci vengono forniti dal fornitore dell'app store nell'ambito del nostro rapporto contrattuale allo scopo di sviluppare ulteriormente la nostra app Myoncare e servizi.

Nel trattamento dei dati operativi, ONCARE agisce in qualità di titolare del trattamento responsabile del trattamento lecito dei dati personali dell'utente.

Tipi di dati: nome, indirizzo e-mail, numero di telefono, data di nascita, data di registrazione, pseudo-chiavi generate dall'app; Token del dispositivo per identificare il dispositivo, il numero di pseudo-identificazione, l'indirizzo IP, il tipo e la versione del sistema operativo utilizzato dal dispositivo.

L'app utilizza l'API di Google Maps per utilizzare le informazioni geografiche. Quando si usa Google Maps, Google raccoglie, elabora e utilizza anche i dati sull'uso delle funzioni della mappa. Informazioni più dettagliate sull'ambito, la base giuridica e lo scopo del trattamento dei dati da parte di Google, nonché il periodo di conservazione, sono disponibili nell'Informativa sulla privacy di Google.

Nella nostra organizzazione, ci assicuriamo che solo le persone che sono obbligate a farlo per adempiere ai loro obblighi contrattuali e legali siano autorizzate a trattare i dati personali. I tuoi dati personali e i dati sanitari che inserisci nella nostra **applicazione myoncare** sarà messo a disposizione del vostro **operatore sanitario** o società

direttamente o tramite un **fornitore di servizi dati** (a seconda del tipo di utilizzo degli **strumenti MyonCare**).

Regole GDPR: Il trattamento dei dati aziendali è giustificato sulla base dell'art. 6 par. 1 lett. b GDPR per l'esecuzione del contratto stipulato con ONCARE ai fini dell'utilizzo dell' **applicazione myoncare**.

GEOLOCALIZZAZIONE IP

Geolocalizzazione IP: Utilizziamo un'applicazione di geolocalizzazione per i nostri Servizi. Utilizziamo ipapi (fornito da apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Vienna, Austria) e Geoapify (fornito da Keptago Ltd., N. Nikolaidi e T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Cipro) per identificare la posizione degli utenti pazienti. Lo utilizziamo per proteggere le nostre applicazioni e per verificare la posizione dell'utente paziente per garantire che l'uso dei nostri servizi sia conforme. Non combiniamo le informazioni che raccogliamo con altre informazioni sull'utente che potrebbero identificarlo. I dati elaborati da apilayer includono l'indirizzo IP del paziente e altri dettagli sulla posizione. La base giuridica per il loro utilizzo è l'art. 6 (1) (f) GDPR. I dati saranno cancellati quando lo scopo associato per il quale sono stati raccolti non esisterà più e non vi sarà più un obbligo legale di conservazione. Per ulteriori informazioni sulla loro politica sulla privacy, consultare <https://ipapi.com/privacy/> e [Informativa sulla privacy | Piattaforma di localizzazione Geoapify](#).

TRATTAMENTO DEI DATI

Applicabile agli utenti dell'app che utilizzano l'app con il proprio medico.

Durante l'utilizzo dell'app myoncare, il tuo **operatore sanitario** inserisce i tuoi dati personali nel portale myoncare per avviare i servizi myoncare (ad es. creazione della cartella clinica, fornitura di un piano di cura individuale, promemoria per l'assunzione di farmaci, ecc.). Inoltre, tu e il tuo **operatore sanitario** può caricare documenti e file sull' **applicazione myoncare** e sul **portale myoncare** e condividerli tra di noi. Il tuo **operatore sanitario** può caricare un'informativa sulla privacy per le tue informazioni e definire altri requisiti di

consenso per te come paziente per i quali deve essere dato il tuo consenso. I file sono archiviati in un database cloud in Germania. Il tuo **operatore sanitario** può consentire la condivisione di tali file con altri **utenti del portale** all'interno della sua istituzione o di altri **fornitori di servizi sanitari** al di fuori del suo istituto (consulente sanitario) per scopi medici. Gli altri utenti del portale non hanno accesso a questi file a meno che l'accesso non sia fornito dall'**operatore sanitario**. Inoltre, il tuo **operatore sanitario** può chiederti di assisterti telefonicamente nella compilazione di questionari (chiamate in uscita). Ciò avviene esclusivamente sotto la direzione del vostro **operatore sanitario** ed esclusivamente da dipendenti autorizzati ONCARE.

Utilizziamo ed elaboriamo le informazioni sanitarie dell'utente solo per le attività operative consentite dall'HIPAA e da altre leggi federali.

Trattiamo tali dati personali, compresi i dati sanitari dell'utente, in base a un accordo con e in conformità con le istruzioni del tuo **operatore sanitario** (accordo sul trattamento dei dati). Ai fini del presente accordo sul trattamento dei dati, l'**operatore sanitario** è responsabile del trattamento dei dati personali e dei dati sanitari dell'utente ai sensi delle leggi applicabili in materia di protezione dei dati in qualità di titolare del trattamento dei dati e ONCARE è il responsabile del trattamento di tali dati personali (sanitari). Ciò significa che ONCARE elabora i dati personali solo in conformità con le istruzioni del **Medico**. In caso di domande o dubbi sul trattamento dei propri dati personali o sanitari, è necessario contattare l'**operatore sanitario** in primo luogo.

TRATTAMENTO DEI DATI SULL'ATTIVITÀ

Applicabile solo se l'utente accetta e attiva il trasferimento dei dati dell'attività tramite gli strumenti myoncare

Strumenti MyonCare offrirvi la possibilità di collegare il **Applicazione myoncare** con alcune app per la salute (ad es. AppleHealth, GoogleFit, Withings) che utilizzi ("**App per la salute**"). Se la connessione viene stabilita dopo che l'utente ha dato il suo consenso, i dati sull'attività raccolti dall'Applicazione Salute saranno messi a disposizione del tuo **operatore sanitario** allo scopo di fornire ulteriori informazioni contestuali sulla tua attività. Al fine di consentire il trattamento dei dati

dell'attività, otterremo preventivamente il tuo consenso al trattamento. Si prega di notare che i dati dell'attività non sono convalidati dagli **strumenti MyonCare** e non deve essere utilizzato dall'**operatore sanitario** a fini diagnostici come base per il processo decisionale medico. Si prega inoltre di notare che i vostri **operatori sanitari** non sono obbligati a verificare i dati della tua attività e non sono tenuti a fornirti alcun feedback in merito ai dati della tua attività.

I dati dell'attività vengono condivisi con il tuo **operatore sanitario** affiliato ogni volta che l'**applicazione myoncare** è accessibile. Puoi revocare il tuo consenso alla condivisione dei dati dell'attività in qualsiasi momento nelle impostazioni dell'**applicazione myoncare**. Si prega di notare che i dati della tua attività non saranno condivisi da questo momento in poi. I dati dell'attività che sono già stati condivisi non verranno eliminati dal **portale myoncare** dei tuoi **operatori sanitari** affiliati.

Il trattamento dei dati relativi all'attività ricade sotto la responsabilità dell'utente.

Tipi di dati: Il tipo e la quantità di dati trasferiti dipendono dalla tua decisione e dai dati disponibili nell'app Salute collegata. I dati possono includere, tra gli altri, peso, altezza, passi effettuati, calorie bruciate, ore di sonno, frequenza cardiaca e pressione sanguigna.

Finalità del trattamento dei dati relativi all'attività: I dati della tua attività saranno messi a disposizione del tuo **operatore sanitario** con cui l'utente è in contatto allo scopo di fornire ulteriori informazioni contestuali sulla sua attività.

Giustificazione del trattamento: Il trattamento dei dati relativi all'attività è sotto la responsabilità dell'utente.

TRATTAMENTO DEI DATI DI SICUREZZA DEI PRODOTTI

Applicabile agli utenti dell'app il cui fornitore di servizi utilizza la variante per dispositivi medici degli strumenti myoncare

L'**applicazione myoncare** è classificato e commercializzato come dispositivo medico secondo le normative europee sui dispositivi medici. In qualità di produttore dell'app, dobbiamo rispettare determinati obblighi legali (ad es. monitoraggio della funzionalità

dell'app, valutazione delle segnalazioni di incidenti che potrebbero essere correlate all'utilizzo dell'app, tracciamento degli utenti, ecc.). Inoltre, l'**applicazione myoncare** permette te e il tuo **operatore sanitario** di comunicare e raccogliere dati personali su determinati dispositivi medici o medicinali utilizzati nel trattamento. I fabbricanti di tali dispositivi medici o medicinali hanno anche obblighi legali in materia di sorveglianza del mercato (ad es. raccolta e valutazione delle segnalazioni di reazioni avverse).

Tipi di dati: segnalazioni di casi, dati personali forniti in una relazione sull'incidente e risultati della valutazione.

Trattamento dei dati sulla sicurezza dei prodotti: Conserveremo e valuteremo tutti i dati personali relativi ai nostri obblighi legali in qualità di produttori di un dispositivo medico e trasmetteremo tali dati personali (se possibile dopo la pseudonimizzazione) alle autorità competenti, agli organismi notificati o ad altri titolari del trattamento dei dati con obblighi di monitoraggio. Inoltre, conserveremo e trasferiremo i dati personali in relazione a dispositivi medici e/o medicinali se riceviamo comunicazioni da parte del tuo **operatore sanitario**, da te in qualità di paziente o da terzi (ad es. i nostri distributori o importatori degli **strumenti MyonCare** nel tuo paese) che devono essere segnalati al produttore del prodotto affinché il produttore possa rispettare i suoi obblighi legali in materia di sicurezza del prodotto.

Regole GDPR

ONCARE è il titolare del trattamento dei dati sulla sicurezza dei prodotti.

La base giuridica per il trattamento dei dati personali per l'adempimento degli obblighi legali in qualità di produttore di dispositivi medici o medicinali è l'art. 9 par. 2 lett. i GDPR in combinato disposto con gli obblighi di monitoraggio esistenti dopo l'immissione in commercio ai sensi della legge sui dispositivi medici e della direttiva sui dispositivi medici (disciplinata dal 26 maggio 2021 nel capitolo VII del nuovo regolamento sui dispositivi medici (UE) 2017/745) e/o della legge sui medicinali.

TRATTAMENTO DEI DATI RELATIVI ALLA GESTIONE DELLA SALUTE IN AZIENDA

Applicabile agli utenti dell'app che utilizzano l'app con la gestione della salute in azienda

Durante l'uso dell'**applicazione myoncare** nell'**azienda** di gestione della salute sul lavoro, alcuni dati personali (sanitari) sono trasmessi in forma aggregata come dati per la gestione della salute in azienda e al **fornitori di servizi dati** commissionato dall'azienda (ad es. analisti di dati o società di ricerca). Né la **società** né alcun **fornitore di servizi dati** può assegnare tali dati alla tua identità. ONCARE raccomanda di non condividere alcun dato personale durante l'uso di **Servizi MyonCare** nell'ambito della gestione della salute in azienda.

Ciò significa che ONCARE e tutti i **fornitori di servizi dati** tratteranno i dati per la gestione della salute sul lavoro solo in conformità con le disposizioni **dell'azienda**. Trattiamo tali dati per la gestione della salute sul lavoro, compresi i vostri dati sanitari, sulla base di un accordo con l'**azienda** e/o un **fornitore di servizi dati** e in conformità con le loro istruzioni. Ai fini del presente Accordo, la Società è il responsabile dei dati e del trattamento dei dati di gestione della salute sul lavoro e ONCARE e qualsiasi **fornitori di servizi dati** ingaggiato dalla tua **azienda**, se presenti, sono i responsabili del trattamento di tali dati. In caso di domande o dubbi sul trattamento dei dati per la gestione della salute sul lavoro, è necessario contattare l'azienda in primo luogo.

Elaborazione dati: Trattiamo i dati di gestione della salute della vostra azienda al fine di poter fornire i nostri **servizi myoncare** per l'**azienda** e per te. I vostri dati di gestione della salute in azienda, che inserite nella nostra **applicazione myoncare**, sarà utilizzato dall'**azienda** (direttamente o tramite un **fornitore di servizi dati**) nell'ambito della gestione della salute sul lavoro. Trattiamo questi dati personali in base a un accordo e in conformità con le istruzioni del tuo **operatore sanitario**. La trasmissione di questi dati di trattamento è pseudonimizzata e crittografata. Per esercitare i propri diritti in qualità di interessato, si prega di contattare il proprio **fornitore di servizi**.

Regole GDPR

I vostri dati per la gestione della salute sul lavoro saranno trattati dalla **società** conformemente alle disposizioni del **GDPR** e tutte le altre normative applicabili in materia di protezione dei dati. La base giuridica per il trattamento

dei dati è, in particolare, il consenso dell'utente ai sensi dell'art. 6 par. 1 lett. a e l'art. 9 par. 2 lett. un **GDPR** o di un'altra norma applicabile alla **società**. Il trattamento dei dati da parte di ONCARE alla **società** (direttamente o tramite un **fornitore di servizi** commissionato dalla **società**) si fonda anche sull'art. 28 **GDPR** (Accordo sul trattamento dei dati).

La **società** in qualità di responsabile dei dati, è responsabile dell'ottenimento del consenso dell'utente, se richiesto dalle norme sulla protezione dei dati, e del trattamento dei dati per finalità di gestione della salute sul lavoro in conformità con le leggi applicabili in materia di protezione dei dati.

QUALI TECNOLOGIE VENGONO UTILIZZATE DAL PORTALE MYONCARE E DALL'APP MYONCARE?

Il **Portale myoncare** funziona come uno strumento basato sul web per il quale è necessaria una connessione Internet funzionante e qualsiasi versione aggiornata del browser Internet Chrome, Firefox o Safari.

Servizio di posta elettronica

Utilizziamo Brevo (fornito da Sendinblue GmbH, con sede in Köpenicker Straße 126, 10179 Berlino) e Sendgrid (fornito da Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Questi servizi di posta elettronica possono essere utilizzati per organizzare l'invio di e-mail. Sendgrid viene utilizzato per inviare e-mail di conferma, conferme di transazioni ed e-mail con informazioni importanti relative alle richieste. I dati inseriti dall'utente per la ricezione delle e-mail vengono memorizzati sui server di Sendgrid. Quando inviamo e-mail per tuo conto tramite SendGrid, utilizziamo una connessione protetta SSL.

La comunicazione tramite posta elettronica viene utilizzata per le attività seguenti:

- Accedere all'applicazione web per la prima volta;
- Workflow per reimpostare la password per l'applicazione web;
- Creare un account per la domanda del paziente;
- Reimpostare la password per l'applicazione del paziente;
- Generazione e invio di un report;

- Sostituire le notifiche push con email per PWA (Progressive Webapp) nei seguenti casi:

- (i) Se un piano di assistenza termina entro un giorno;
- (ii) se il farmaco è stato assegnato;
- (ii) quando l'Informativa sulla privacy è stata aggiornata;
- (iv) quando un appuntamento viene inviato a pazienti e medici, in particolare per il tipo di appuntamento "videochiamata";
- (v) Tutte le informazioni su un **compito di cura** o quando un **operatore sanitario** ha assegnato un **compito di cura**.

Brevo (Informativa sulla privacy):

Informativa sulla privacy - Protezione dei dati personali | Brevo

SendGrid (Informativa sulla privacy):

<https://sendgrid.com/resource/general-data-protection-regulation-2/>.

Matomo

Questo è uno strumento di analisi web open source. Matomo (fornito da InnoCraft Ltd., Nuova Zelanda) non trasmette dati a server al di fuori del controllo di ONCARE. Matomo è inizialmente disabilitato quando si utilizzano i nostri servizi. Solo se sei d'accordo, il tuo comportamento utente verrà registrato in forma anonima. Se disattivato, verrà memorizzato un "cookie persistente", a condizione che le impostazioni del browser lo consentano. Questo cookie segnala a Matomo che non si desidera che il browser venga registrato.

Le informazioni sull'utilizzo raccolte dal cookie vengono trasmesse ai nostri server e lì memorizzate in modo da poter analizzare il comportamento dell'utente.

Le informazioni generate dal cookie sull'utilizzo da parte dell'utente sono:

- Ruolo utente;
- Geolocalizzazione dell'utente;
- Browser;
- Utente-OS;
- Indirizzo IP;
- Siti visitati via web/PWA (per maggiori informazioni, si veda la sezione relativa alle PWA nella presente Privacy Policy);
- pulsanti su cui l'utente fa clic nel **portale myoncare** nell'**applicazione myoncare** e nel **myoncare PWA**;
- tempo in cui l'utente ha utilizzato il contenuto.

Le informazioni generate dal cookie non saranno trasmesse a terzi.

È possibile rifiutare l'uso dei cookie selezionando le impostazioni appropriate nel browser. Tuttavia, tieni presente che in questo caso potresti non essere in grado di utilizzare tutte le funzionalità. Per ulteriori informazioni, consultare: <https://matomo.org/privacy-policy/>.

La base giuridica per il trattamento dei dati personali degli utenti è l'art. 6 par. 1 frase 1 lett. a GDPR. Il trattamento dei dati personali degli utenti ci consente di analizzare il comportamento di utilizzo. Valutando i dati ottenuti, possiamo raccogliere informazioni sull'utilizzo dei singoli componenti dei nostri servizi. Questo ci aiuta a migliorare continuamente i nostri servizi e la loro usabilità.

Trattiamo e conserviamo i dati personali solo per il tempo necessario a soddisfare lo scopo previsto.

TRASFERIMENTO SICURO DEI DATI PERSONALI

Adottiamo misure di sicurezza tecniche e organizzative adeguate per proteggere in modo ottimale i dati personali da noi memorizzati contro la manipolazione accidentale o intenzionale, la perdita, la distruzione o l'accesso da parte di persone non autorizzate. I livelli di sicurezza vengono continuamente verificati in collaborazione con esperti di sicurezza e adattati ai nuovi standard di sicurezza.

Lo scambio di dati da e verso l'app è crittografato. Utilizziamo TLS e SSL come protocolli di crittografia per il trasferimento sicuro dei dati. Anche lo scambio di dati è crittografato e viene effettuato con pseudo-chiavi.

TRASFERIMENTI DI DATI / DIVULGAZIONE A TERZI

Trasmetteremo i vostri dati personali a terzi solo nell'ambito delle disposizioni di legge o sulla base del vostro consenso. In tutti gli altri casi, le informazioni non saranno divulgate a terzi, a meno che non siamo obbligati a farlo a causa di norme legali obbligatorie (divulgazione a organismi esterni, comprese le autorità di vigilanza o di polizia). Qualsiasi trasmissione di dati personali viene crittografata durante la trasmissione.

Condivideremo le informazioni e i dati sull'utente solo se richiesto dallo Stato o dagli Stati Uniti. legge federale; ciò include le richieste del Dipartimento della Salute e dei Servizi Umani se l'agenzia desidera verificare la conformità con gli Stati Uniti legge federale. Possiamo anche elaborare e condividere i tuoi dati sanitari al fine di:

- conformità alle leggi federali, statali o locali;
- Fornire supporto per le attività di sanità pubblica, come la malattia o l'uso di attrezzature mediche;
- fornire alle autorità informazioni per proteggere le vittime di abusi o negligenza;
- Conformità con le attività di supervisione sanitaria federale e statale, come le indagini sulle frodi;
- Per far rispettare le forze dell'ordine o le ordinanze del tribunale, le citazioni in giudizio o altre azioni sovrane correlate;
- Condurre ricerche sui protocolli di revisione interna per garantire un equilibrio tra privacy ed esigenze di ricerca;
- Evitare una grave minaccia per la salute o la sicurezza.

INFORMAZIONI GENERALI SUL CONSENSO AL TRATTAMENTO DEI DATI

Il consenso dell'utente costituisce anche il consenso al trattamento dei dati ai sensi della legge sulla protezione dei dati. Prima di concedere il tuo consenso, ti informeremo sullo scopo del trattamento dei dati e sul tuo diritto di opposizione. Se il consenso riguarda anche il trattamento di categorie particolari di dati personali, l'**applicazione myoncare** vi informerà espressamente di ciò nell'ambito della procedura di consenso.

Per il trattamento dei dati per il quale è richiesto il consenso dell'utente (come spiegato nel presente **Informativa sulla privacy**), il consenso sarà ottenuto nell'ambito del processo di registrazione. Dopo l'avvenuta registrazione, i consensi possono essere gestiti nelle impostazioni dell'account del **Applicazione myoncare**.

Regole GDPR

Trattamento di categorie particolari di dati personali ai sensi dell'art. 9 par. 1 GDPR può avvenire solo se ciò è richiesto dalla legge e non vi è motivo di presumere che i tuoi legittimi interessi precludano il trattamento di questi dati personali o che tu abbia dato il tuo consenso

al trattamento di questi dati personali ai sensi dell'art. 9 par. 2 del GDPR.

DESTINATARI DEI DATI / CATEGORIE DI DESTINATARI

Nella nostra organizzazione, ci assicuriamo che solo le persone siano autorizzate a trattare i dati personali necessari per adempiere ai loro obblighi contrattuali e legali. I tuoi dati personali e i dati sanitari che inserisci nella nostra **applicazione myoncare** saranno messi a disposizione del tuo **operatore sanitario** e/o **società** direttamente o tramite un **fornitore di servizi dati** (a seconda del tipo di utilizzo degli **strumenti myoncare**). In alcuni casi, i fornitori di servizi supportano i nostri reparti specializzati nell'adempimento dei loro compiti. I necessari accordi sulla protezione dei dati sono stati stipulati con tutti i fornitori di servizi che sono responsabili del trattamento dei dati personali. Questi fornitori di servizi sono Google (Google Firebase), Fornitori di servizi di archiviazione cloud e servizi di supporto.

Google Firebase è un "database NoSQL" che consente la sincronizzazione tra il **portale myoncare del tuo operatore sanitario** e l' **applicazione myoncare**. NoSQL definisce un meccanismo per l'archiviazione dei dati che non è solo modellato in relazioni tabulari, consentendo una scalabilità "orizzontale" più semplice rispetto ai sistemi di gestione di database tabulari/relazionali in un cluster di macchine.

A questo scopo, una pseudo-chiave dell' **applicazione myoncare** viene memorizzato in Google Firebase insieme al piano di assistenza corrispondente. Il trasferimento dei dati è pseudonimizzato per ONCARE e i suoi fornitori di servizi, il che significa che ONCARE e i suoi fornitori di servizi non possono stabilire una relazione con l'utente in qualità di interessato. Ciò si ottiene crittografando i dati durante il trasferimento tra l'utente e il suo **operatore sanitario** o **società** (direttamente o a qualsiasi **fornitore di servizi dati**) e utilizzando pseudo-chiavi invece di identificatori personali come il nome o l'indirizzo e-mail per tracciare questi trasferimenti. La re identificazione avviene non appena i dati personali hanno raggiunto l'account del tuo **operatore sanitario** o **società** nel **portale myoncare** o il tuo account nella sezione **applicazione myoncare**, dopo che è stato verificato da token specifici.

I nostri fornitori di cloud storage offrono una gamma di servizi di spazio cloud in cui il Firebase manager, che gestisce gli URL Firebase per il **portale myoncare**, viene memorizzato. Inoltre questi fornitori di servizi forniscono il dominio del server isolato del **portale myoncare**, in cui sono memorizzati i dati personali dell'utente. Ospita anche i servizi di gestione video e file di myoncare, che consentono videoconferenze crittografate tra l'utente e il suo **Medico** così come lo scambio di file. Accesso ai tuoi dati personali da parte tua e del tuo **operatore sanitario** è garantito dall'invio di token specifici. Questi dati personali sono crittografati durante il trasferimento e a riposo e pseudonimizzati per ONCARE e i suoi fornitori di servizi. I fornitori di servizi ONCARE non hanno mai accesso a questi dati personali.

Inoltre, ci avvaliamo di fornitori di servizi per elaborare le richieste di servizio (fornitori di servizi di supporto) relative all'utilizzo dell'account, ad esempio se hai dimenticato la password, desideri modificare il tuo indirizzo e-mail memorizzato, ecc. Con questi fornitori di servizi sono stati stipulati i necessari accordi per l'elaborazione degli ordini; Inoltre, i dipendenti incaricati dell'elaborazione delle richieste di servizio sono stati formati di conseguenza. Al ricevimento della richiesta di servizio, le verrà assegnato un numero di biglietto.

Se si tratta di una richiesta di servizio relativa all'utilizzo dell'account, le informazioni pertinenti che ci hai fornito quando ci hai contattato saranno inoltrate a uno dei dipendenti autorizzati del servizio esterno. Ti contatteranno quindi.

In caso contrario, rimarranno trattati da personale ONCARE appositamente autorizzato, come descritto nella sezione "TRATTAMENTO DEI DATI OPERATIVI".

Attraverso i nostri fornitori di servizi di supporto, utilizziamo lo strumento RepairCode, noto anche come Digital Twin Code, che è una piattaforma di customer experience per la gestione di feedback esterni con la possibilità di creare ticket di supporto. Qui troverai il
Informativa sulla privacy:
<https://app.repaircode.de/?main=main-client> –
[Legale/privacy](#).

Infine, mostriamo contenuti da Instagram (fornitore: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublino 2, Irlanda), come immagini, video o post. Se fai clic su un post di Instagram

collegato, verrai reindirizzato a Instagram. Durante questo processo, Instagram può impostare cookie ed elaborare i dati dell'utente.

Quando visiti una pagina contenente un post di Instagram collegato, il tuo browser potrebbe stabilire automaticamente una connessione ai server di Instagram. In questo modo Instagram riceve l'informazione che l'utente ha visitato il nostro sito web, anche se non dispone di un account Instagram o non ha effettuato l'accesso. Se hai effettuato l'accesso, Instagram potrebbe associare la visita al tuo account utente.

Informativa sulla privacy:

<https://privacycenter.instagram.com/policy>

TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI

Per fornire i nostri servizi, possiamo avvalerci di fornitori di servizi situati al di fuori dell'Unione Europea (paese terzo). Se i dati vengono trasferiti in un paese terzo in cui il livello di protezione dei dati personali è ritenuto inadeguato, ci assicuriamo che vengano adottate misure adeguate in conformità con il diritto nazionale ed europeo. Se necessario, ciò include l'attuazione di clausole contrattuali standard tra le parti del trattamento.

I dati personali saranno trasferiti in paesi terzi solo se ciò è necessario per l'adempimento dell'obbligo contrattuale, è richiesto dalla legge o se l'utente ci ha fornito il suo consenso.

La sincronizzazione dell' **applicazione myoncare** e il **portale myoncare** avviene tramite Google Firebase. Il server di Google Firebase è ospitato nell'Unione Europea. Tuttavia, come descritto nei Termini di utilizzo di Google Firebase, sono possibili trasferimenti di dati a breve termine verso i paesi in cui si trovano Google o i suoi fornitori di servizi; per alcuni servizi di Google Firebase, i dati vengono trasferiti solo negli Stati Uniti, a meno che l'elaborazione non avvenga nell'Unione Europea o nello Spazio economico europeo. L'accesso illegale ai tuoi dati è impedito dalla crittografia end-to-end e dai token di accesso sicuri. I nostri server sono ospitati in Germania. A scopo di analisi, le e-mail inviate con SendGrid contengono un cosiddetto "pixel di tracciamento" che si connette ai server di Sendgrid quando l'e-mail viene aperta. Questa funzione può

essere utilizzata per determinare se un messaggio di posta elettronica è stato aperto.

Integriamo i contenuti di Instagram, forniti da Meta Platforms Ireland Ltd. Se si fa clic su un post di Instagram collegato, è possibile che i dati personali (ad es. indirizzo IP, informazioni sul browser, interazioni) vengano trasmessi a Meta Platforms Inc. negli Stati Uniti o in altri paesi terzi.

Meta è certificata ai sensi dell'accordo UE-USA Data Privacy Framework (DPF), che riconosce un livello adeguato di protezione dei dati per i trasferimenti negli Stati Uniti. Tuttavia, i dati possono essere trasferiti anche in paesi per i quali non esiste una decisione di adeguatezza da parte della Commissione europea. In tali casi, possono essere necessarie ulteriori misure di protezione, sebbene la loro efficacia non possa sempre essere pienamente garantita.

GDPR - Regole

Il trattamento dei dati si basa sul consenso dell'utente (art. 6 par. 1 lett. un GDPR). Puoi revocare il consenso in qualsiasi momento. La revoca rimane inalterata dalla liceità delle operazioni di trattamento dei dati già avvenute.

Si prega di notare che i dati dell'utente vengono solitamente trasmessi da noi a un server di SendGrid negli Stati Uniti e lì memorizzati. Abbiamo stipulato un contratto con Sendgrid che contiene le clausole contrattuali standard dell'UE. Ciò garantisce un livello di protezione paragonabile a quello dell'UE.

Per elaborare i dati delle attività, all'interno del sito vengono utilizzate interfacce con i servizi Google Cloud (nel caso di GoogleFit) o con AppleHealth o Withings all'interno dei dispositivi mobili degli **utenti dell'app**. **Strumenti MyonCare** utilizzare queste interfacce, fornite da Google, Apple e Withings, per richiedere i dati dell'attività dalle app per la salute connesse. La richiesta inviata dagli **strumenti myoncare** non contiene dati personali. I dati personali sono messi a disposizione degli **strumenti myoncare** tramite queste interfacce.

DURATA DELLA CONSERVAZIONE DEI DATI PERSONALI IN CONFORMITÀ CON IL GDPR

Conserviamo i tuoi dati personali per tutto il tempo necessario allo scopo per il quale sono stati trattati. Si prega di notare che numerosi periodi di conservazione

richiedono la conservazione continua dei dati personali. Ciò vale in particolare per gli obblighi di ritenzione previsti dal diritto commerciale o fiscale (ad es. codice commerciale, legge fiscale, ecc.). Inoltre, il tuo **operatore sanitario** deve inoltre garantire la conservazione delle cartelle cliniche (tra 1 e 30 anni, a seconda del tipo di documenti).

Inoltre, e solo se il tuo **operatore sanitario** utilizza la variante del dispositivo medico degli **strumenti MyonCare**, si applicano determinati periodi di conservazione derivanti dalla legge sui dispositivi medici a causa della classificazione dell'**applicazione myoncare** come dispositivo medico. Si prega di notare che ONCARE è inoltre soggetta a obblighi di conservazione concordati contrattualmente con l'**operatore sanitario** sulla base delle disposizioni di legge. Se non vi sono altri obblighi di conservazione, i dati personali saranno regolarmente cancellati non appena lo scopo è stato raggiunto.

Inoltre, possiamo conservare i dati personali se l'utente ci ha dato il suo consenso a farlo o se sorge un contenzioso e utilizziamo le prove entro i termini di prescrizione previsti dalla legge, che possono arrivare fino a 30 anni; Il termine di prescrizione regolare è di tre anni.

TRASFERIMENTI DI DATI PERSONALI

Diversi dati personali sono necessari per l'instaurazione, l'esecuzione e la cessazione del rapporto contrattuale e l'adempimento dei relativi obblighi contrattuali e di legge. Lo stesso vale per l'uso della nostra **applicazione myoncare** e le varie funzioni che offre.

Abbiamo riassunto i dettagli per te al punto precedente. In alcuni casi, i dati personali devono essere raccolti o resi disponibili anche in conformità con le disposizioni di legge. Si prega di notare che senza fornire questi dati personali, non è possibile elaborare la richiesta o adempiere all'obbligo contrattuale sottostante.

DIRITTI DI ACCESSO

Affinché l'**applicazione myoncare** per funzionare sul tuo dispositivo, l'app deve ricevere varie autorizzazioni per accedere a determinate funzioni del dispositivo. Per tutti i dispositivi, indipendentemente dal sistema operativo utilizzato, è necessario concedere all'app determinate autorizzazioni, che chiamiamo "diritti di accesso di base". Se applicabile, li elencheremo in ordine di sistema

operativo (Android o iOS) in base alle "condizioni di base". A seconda del sistema operativo del dispositivo che stai utilizzando, potrebbe avere funzionalità aggiuntive che richiedono autorizzazioni aggiuntive per il funzionamento dell'app.

I diritti di accesso di base (Android e iOS) sono:

Ottieni connessioni Wi-Fi

Necessario per garantire la funzionalità del download dei documenti in combinazione con le connessioni Wi-Fi.

Ottieni connessione di rete

Necessario per garantire la funzionalità del download dei documenti in combinazione con connessioni di rete che non sono connessioni Wi-Fi.

Disattiva il blocco schermo (impedisce la modalità stand-by)

Necessario affinché i video che appartengono ai documenti forniti possano essere riprodotti direttamente nell'app senza essere interrotti da un blocco schermo.

Accesso a tutte le reti

L'accesso a tutte le reti è necessario per scaricare i documenti.

Disattiva la modalità di sospensione

Ciò è necessario affinché i video che appartengono ai documenti forniti possano essere riprodotti direttamente nell'app senza che la riproduzione venga interrotta dal verificarsi dell'ibernazione.

Dati mobili / Accesso ai dati mobili

Se l'utente desidera scaricare i documenti esclusivamente tramite Wi-Fi, può effettuare l'impostazione appropriata nel menu dell'app e disattivare l'uso dei dati mobili. L'accesso ai dati mobili è necessario per garantire la funzionalità di disabilitazione dei download di documenti sui dati mobili.

Accesso alla telecamera

L'accesso alla fotocamera è necessario per la scansione dei codici QR e per le consultazioni video.

Accesso al microfono

Per le consultazioni video è necessario l'accesso al microfono.

Accedere a file e foto

Ciò è necessario per lo scambio di file tra l'utente e gli utenti del portale collegati.

Accesso ai browser web

Questa operazione è necessaria per visualizzare i file ricevuti dagli utenti del portale connessi.

Utilizziamo le notifiche push, che sono messaggi che vengono inviati al tuo dispositivo mobile come servizio dell' **applicazione myoncare** tramite servizi come Apple Push Notification Service o Google Cloud Messaging Service. Questi servizi sono funzionalità standard dei dispositivi mobili. L'Informativa sulla privacy del Fornitore di servizi disciplina l'accesso, l'uso e la divulgazione delle informazioni personali a seguito dell'utilizzo di questi servizi da parte dell'utente.

DECISIONI AUTOMATIZZATE IN SINGOLI CASI IN CONFORMITÀ CON IL GDPR

Per prendere decisioni utilizziamo un'elaborazione totalmente automatizzata.

I DIRITTI DELL'UTENTE PREVISTI DALL'HIPAA

Sotto **HIPAA**, l'utente dispone dei seguenti diritti:

- Visualizzare e copiare alcune parti delle informazioni sanitarie. L'utente può richiedere che i propri dati sanitari siano messi a disposizione in formato elettronico. Una copia o un riepilogo delle tue informazioni sanitarie ti verrà fornito, di solito entro 30 giorni dalla tua richiesta. Potrebbe essere addebitata una ragionevole commissione di elaborazione.

- Puoi richiedere che il contenuto delle tue informazioni sanitarie venga modificato se ritieni che le informazioni sanitarie siano errate o incomplete. È possibile richiedere la correzione delle informazioni sanitarie se si ritiene che siano inesatte o incomplete.

- Stabilire la divulgazione obbligatoria delle informazioni sanitarie per gli ultimi sei anni, con restrizioni su trattamento, rimborso e trattamento. Potrebbe essere addebitata una ragionevole commissione di elaborazione.

- Puoi richiedere che alcune informazioni sanitarie che includono trattamenti, pagamenti di royalty o altri argomenti medici non vengano utilizzate o condivise.

- L'utente può richiedere una copia cartacea dell'Informativa sulla privacy in qualsiasi momento, anche se ha accettato di ricevere l'avviso solo in formato elettronico.

- Presentare un reclamo all'autorità competente se si ritiene che i propri diritti in materia di protezione dei dati siano stati violati. L'utente può presentare un reclamo agli Stati Uniti. Dipartimento della Salute e dei Servizi Umani inviando una lettera a 200 Independence Avenue, S.W., Washington, D.C. 20201, telefonicamente al numero 1-800-368-1019 (numero verde) o 1-800-537-7697 (TTD), oppure visitando <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>.

Molti Stati Uniti Gli stati hanno emanato le proprie leggi per proteggere i diritti dei pazienti, che si applicano ai pazienti di medici e/o ospedali e altre strutture sanitarie. Alcuni di questi Stati Uniti Gli stati richiedono ai medici di fornire una copia di questi diritti dei pazienti ai loro pazienti.

I TUOI DIRITTI IN QUALITÀ DI INTERESSATO AI SENSI DEL GDPR

Desideriamo informarvi sui vostri diritti in qualità di interessati. Tali diritti sono stabiliti negli articoli da 15 a 22 del GDPR e comprendono:

Diritto all'informazione (art. 15 GDPR): L'utente ha il diritto di richiedere informazioni sull'eventuale e sulle modalità di trattamento dei propri dati personali, comprese le informazioni sulle finalità del trattamento, i destinatari, il periodo di conservazione e i diritti di rettifica, cancellazione e opposizione. L'utente ha inoltre il diritto di ricevere una copia di tutti i dati personali in nostro possesso.

Diritto alla cancellazione / diritto all'oblio (Art. 17 GDPR): L'utente può chiederci di cancellare i propri dati personali raccolti e trattati da noi senza ingiustificato ritardo. In questo caso, ti chiederemo di eliminare l' **applicazione myoncare** compreso il tuo UID (numero di identificazione univoco) dal tuo smartphone/telefono cellulare.

Diritto di rettifica (art. 16 GDPR): L'utente può chiederci di aggiornare o correggere i dati personali inesatti o di completare i dati personali incompleti.

Diritto alla portabilità dei dati (art. 20 GDPR): In linea di principio, l'utente può richiedere la fornitura di dati personali che ci ha fornito e che vengono elaborati automaticamente sulla base del suo consenso o dell'esecuzione di un contratto con l'utente in forma leggibile da una macchina, in modo che possano essere "trasferiti" a un fornitore di servizi sostitutivo.

Diritto di limitazione del trattamento dei dati (art. 18 GDPR): L'utente ha il diritto di richiedere la limitazione del trattamento dei propri dati personali se l'esattezza dei dati è contestata, se il trattamento è illecito, se i dati sono necessari per rivendicazioni legali o se è in corso un'obiezione al trattamento.

Diritto di opposizione al trattamento dei dati (art. 21 GDPR): L'utente ha il diritto di opporsi all'utilizzo dei propri dati personali da parte nostra e di revocare il proprio consenso in qualsiasi momento se trattiamo i suoi dati personali sulla base del suo consenso. Continueremo a fornire i nostri servizi se non dipendono dalla revoca del consenso.

Per esercitare tali diritti, si prega di contattare il proprio **operatore sanitario** o **società** in prima istanza o contattateci all'indirizzo: privacy@myoncare.com. Ti chiederemo di fornire una prova sufficiente della tua identità per garantire che i tuoi diritti siano protetti e che i tuoi dati personali saranno divulgati solo a te e non a terzi.

Vi preghiamo di contattarci in qualsiasi momento all'indirizzo privacy@myoncare.com. Se avete domande sul trattamento dei dati nella nostra azienda o se desiderate revocare il vostro consenso. L'utente ha inoltre il diritto di contattare l'autorità di controllo competente per la protezione dei dati.

INVIA UN RECLAMO

Se l'utente ritiene che la propria privacy sia stata violata da ONCARE, può presentare un reclamo a noi e agli Stati Uniti Segretario alla Salute e ai Servizi Umani a Washington, D.C. Non ci sono svantaggi per te nel presentare un reclamo. Per presentare un reclamo o

ricevere ulteriori informazioni, si prega di utilizzare le seguenti opzioni di contatto:

Telefono: +49 (0) 89 4445 1156

E-mail: privacy@myoncare.com

Indirizzo: Balanstraße 71a
81541 Monaco di Baviera, Germania

Re: Reclamo

- Presentare un reclamo se ritiene che i suoi diritti di privacy siano stati violati. Dipartimento della Salute e dei Servizi Umani, scrivere a 200 Independence Ave., S.W., Washington, D.C. 20201 o chiama il numero 1-800-368-1019 (numero verde) o 1-800-537-7697 (TTD) o presenta un reclamo online all'indirizzo <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

RESPONSABILE DELLA PROTEZIONE DEI DATI AI SENSI DEL GDPR

Il nostro responsabile della protezione dei dati è a disposizione per rispondere a tutte le domande sulla protezione dei dati all'indirizzo privacy@myoncare.com.

LIMITE DI ETÀ DELLA DOMANDA

È necessaria un'età minima di 18 anni per utilizzare l'App myoncare. Se hai meno di 18 anni, il tuo genitore o tutore deve fornire il consenso alla privacy necessario per utilizzare l'app.

MODIFICHE ALL'INFORMATIVA SULLA PRIVACY

Ci riserviamo espressamente il diritto di modificare la presente Informativa sulla privacy in futuro a nostra esclusiva discrezione. Modifiche o aggiunte possono essere necessarie, ad esempio, per soddisfare i requisiti giuridici, per conformarsi agli sviluppi tecnici ed economici o per soddisfare gli interessi di **app** o **Utenti del portale**.

Le modifiche sono possibili in qualsiasi momento e saranno comunicate all'utente in modo appropriato e in un lasso di tempo ragionevole prima che diventino effettive (ad esempio, pubblicando un'Informativa sulla privacy rivista al momento dell'accesso o fornendo un preavviso di modifiche sostanziali).

ONCARE GmbH

Indirizzo postale

Balanstraße 71a
81541 Monaco, Germania

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Informazioni di contatto del responsabile della
protezione dei dati
privacy@myoncare.com

Ultimo aggiornamento il 20 febbraio 2025

* * * *