# PIATTAFORMA MYONCARE – FORNITORE DI SERVIZI PER L'INFORMATIVA SULLA PRIVACY A PARTIRE DA GIUGNO 2025

Benvenuti su myoncare, il portale sanitario digitale per un'assistenza efficiente e basata sulle esigenze dei pazienti.
Per noi di Oncare GmbH (di seguito denominati "**ONCARE"** oppure "**noi**", "**Noi**", "**nostro**"), la protezione della tua privacy e di tutti i dati personali che ti riguardano durante l'utilizzo del portale myoncare è di grande importanza e importanza. Siamo consapevoli della responsabilità che deriva dalla fornitura e dalla conservazione dei tuoi dati personali nel portale myoncare (= piattaforma). 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.

La presente Informativa sulla privacy si compone di due parti:

• La prima parte contiene le norme sulla protezione dei dati per l'utilizzo della piattaforma myoncare in Europa sulla base del Regolamento generale sulla protezione dei dati (GDPR).
• La seconda parte contiene disposizioni supplementari in conformità con i requisiti della legge statunitense sulla protezione dei dati (HIPAA). Questi si applicano in particolare **se i dati sanitari sono trattati da un'entità coperta dagli Stati Uniti o se i fornitori di servizi operano nell'ambito del sistema sanitario statunitense** – indipendentemente dalla residenza dell'interessato.

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. Nella presente Informativa sulla privacy, scoprirai perché e come **ONCARE** Elabora i dati personali dell'utente che raccogliamo dall'utente o che l'utente ci fornisce quando decide di utilizzare il portale myoncare. In particolare, troverete una descrizione del tipo di dati personali che raccogliamo e trattiamo, nonché lo scopo e la base su cui trattiamo i dati personali; Inoltre, qui troverete 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, avrai la possibilità di acconsentire all'Informativa sulla privacy e acconsentire al trattamento dei tuoi dati personali 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.

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

## 1. DEFINIZIONI

**"Utente App"** indica qualsiasi utente dell'app myoncare (il tuo paziente).
**"Tecnologia blockchain"** Il sistema myoncare contiene un database aggiuntivo in cui sono memorizzati i dati di tutte le installazioni.
**"Fornitore del piano di assistenza"** indica l'utente o qualsiasi altro fornitore di servizi o terza parte (ad esempio, produttore di dispositivi medici, azienda farmaceutica) che rende disponibili i Piani di assistenza ad altri utenti del Portale attraverso il Negozio myonclinic o altri mezzi di scambio di dati.
**"Utente Careplan"** indica l'utente o un altro fornitore di servizi (Utente del Portale) che utilizza un Piano di Cura ("Percorso") per il trattamento dei suoi Pazienti Registrati.
**"Percorso"** è un piano di trattamento standardizzato composto da più attività di cura, possibilmente sequenziate tra loro nel tempo, che possono determinare le fasi per la diagnosi e le terapie.
**"Compiti di cura"** sono compiti o azioni specifiche all'interno di un percorso che devono essere svolte dai prestatori di cura coinvolti, dal personale infermieristico o dal paziente stesso.
"**Provider**" indica l'utente o qualsiasi altro medico, clinica, struttura sanitaria o altro operatore sanitario che agisce da solo o per conto dell'utente o di un altro medico, clinica o struttura sanitaria (Utente previsto).
"**Applicazione myoncare**" indica l'applicazione mobile myoncare per i pazienti che desiderano utilizzare i servizi offerti da ONCARE attraverso l'App.
"**Negozio myonclinic**" è la piattaforma gestita da **ONCARE** Fornisce concetti di assistenza digitale (piani di trattamento) per il trattamento dei pazienti registrati tramite il portale Myoncare.
"**Strumenti myoncare**" indica l'app myoncare e il portale myoncare insieme.
"**myoncare PWA**" indica l'applicazione myoncare Progressive Web App per i pazienti che desiderano utilizzare i servizi offerti da ONCARE tramite la 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.
"**ONCARE"** significa ONCARE GmbH, Germania.
"**Utente del portale**" indica l'utente o un altro fornitore di servizi che utilizza il portale myoncare basato sul web.
"**Informativa sulla privacy dei pazienti**" indica l'Informativa sulla privacy che descrive la raccolta, l'uso e la conservazione delle informazioni personali (sanitarie) dei Pazienti che utilizzano l'App myoncare. 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.
"**Informativa sulla privacy**" indica la presente informativa fornita all'utente in qualità di utente del Portale myoncare, che descrive le modalità di raccolta, utilizzo e archiviazione dei dati personali dell'utente e lo informa dei suoi ampi diritti.
"**Termini** "di utilizzo" indica i termini e le condizioni d'uso per l'utilizzo del Portale myoncare.

## 2. TRATTAMENTO DEI DATI

Oncare GmbH, una società registrata presso il Tribunale distrettuale di Monaco di Baviera con numero di registrazione 219909 con sede legale in Balanstraße 71a, 81541 Monaco di Baviera, Germania, offre e gestisce il portale web interattivo myoncare Portal (per gli operatori sanitari) e l'applicazione mobile myoncare App (per i pazienti) come accesso ai servizi myoncare. Questo **Informativa sulla privacy** si applica a tutti i dati personali trattati da ONCARE in relazione all'utilizzo del **Portale myoncare** . Per l'uso del **Applicazione myoncare** dai pazienti, puoi trovare un Informativa sulla privacy per i pazienti qui: https://www.myoncare.com/privacy-policy

## 3. CHE COSA SONO I DATI PERSONALI

"**Dati personali**" indica qualsiasi informazione che consente di identificare una persona fisica. Ciò include, a titolo esemplificativo ma non esaustivo, nome, data di nascita, indirizzo, numero di telefono, indirizzo e-mail e indirizzo IP.

"**Dati sanitari**" indica i dati personali relativi alla salute fisica e mentale di una persona fisica, compresa la fornitura di servizi sanitari che divulgano 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, "**pseudonimizzato**l dati 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 reidentificati dalla chiave di identificazione. (ai sensi dell'art. 4 n. 5 GDPR).

**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 sul browser. La PWA si basa sulla tecnologia di "React". React" è un software open source per applicazioni PWA.
Per utilizzare il **myoncare PWA** funzione, i pazienti hanno bisogno di un computer o smartphone e di una connessione Internet attiva. Non è necessario scaricare un'app.

Le seguenti informazioni sul **Applicazione myoncare** si applica anche al **myoncare PWA**, se non diversamente descritto in questa sezione.

**4. QUALI DATI PERSONALI VENGONO UTILIZZATI QUANDO SI UTILIZZA L'APP MYONCARE?**

Possiamo elaborare le seguenti categorie di dati su di te quando utilizzi il **Applicazione myoncare** :

**Dati operativi:** Dati personali che ci fornisci al momento della registrazione sul nostro **Portale myoncare**, contattandoci in merito a problemi con il portale o interagendo in altro modo con noi ai fini dell'utilizzo del portale.

**Dati del trattamento**: Raccogli i dati personali dei tuoi pazienti, come nome, età, altezza, peso, indicazione, sintomi di malattia e altre informazioni in relazione al trattamento dei tuoi pazienti (ad es. in un piano di cura) nel **Portale myoncare**. I dati sull'attività dei pazienti connessi sono messi a disposizione dell'utente nel **Portale myoncare** .

**Dati del negozio commerciale:** Dati del Negozio Commerciale: Dati personali trattati in relazione all'utilizzo del Negozio myonclinic, in particolare in relazione alla paternità, alla configurazione o all'acquisto di piani di trattamento digitali ("Percorsi"). Il negozio è gestito da myon.clinic GmbH, una filiale di Oncare GmbH. L'utilizzo del Negozio richiede l'elaborazione del tuo nome, dei dati di contatto professionali e, se applicabile, dei dati di pagamento (solo per i contenuti a pagamento). Oncare GmbH elabora questi dati esclusivamente per la fornitura tecnica delle funzioni della piattaforma e non per i propri scopi commerciali.

**Dati relativi all'attività:** Dati personali da noi trattati quando un **L'utente dell'app si connette** Le **Applicazione myoncare** a un'applicazione sanitaria (ad es. AppleHealth, GoogleFit, Withings). I dati sull'attività dei pazienti connessi sono messi a disposizione dell'utente nel **Portale myoncare**.

**Analisi dei dati di utilizzo anonimizzati per il miglioramento della piattaforma:**
Trattiamo solo dati tecnici di utilizzo anonimizzati e non personali (ad es. informazioni aggregate sulla frequenza di utilizzo o sulle prestazioni del sistema) per sviluppare ulteriormente la funzionalità e l'esperienza utente del portale. Questi dati non contengono informazioni identificative e non consentono di trarre conclusioni sui singoli utenti del portale. I dati personali degli operatori sanitari non vengono elaborati per scopi di ricerca o commerciali.

**Dati provenienti da produttori di dispositivi o laboratori:**
Inoltre, i dati personali possono essere trattati dai produttori di dispositivi medici connessi o dai fornitori di servizi di laboratorio nell'ambito di processi di assistenza integrata, a condizione che siano commissionati o utilizzati dal fornitore di servizi tramite il portale myoncare.

**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 nel caso in cui l'utente segnali un incidente, al fine di garantire la certezza del diritto o la vigilanza delle aziende farmaceutiche o dei dispositivi medici.

**Dati di rimborso:** Dati personali necessari per il processo di rimborso.

**5. TECNOLOGIA BLOCKCHAIN**

Blockchain **Tecnologia** ("**Blockchain**") (brevetto europeo n. 4 002 787) è un **opzionale** servizio non obbligatorio. Dipende da te, il **fornitore di servizi**, per 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 progetti di blockchain.

Le **Blockchain** Nel sistema MyonCare è presente un database aggiuntivo in cui sono memorizzati i dati dell'applicazione. Tutti i dati della blockchain **è** conservato 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.
Le **Blockchain** Generalmente 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, quindi le transazioni e le modifiche alle informazioni possono essere ricondotte 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 rimanga 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 cambierà e il collegamento a quel blocco andrà perso. Se tutti i nodi (nodi della rete) tentano di sincronizzare le proprie copie, viene determinato che la copia modificata è stata modificata e la rete considera tale nodo non integro. Questo processo tecnico impedisce a persone non autorizzate di manipolare i contenuti della catena blockchain.

La nostra **Blockchain** è una **Blockchain privata**. Una **Blockchain** privata è decentralizzata. Si tratta di un cosiddetto sistema di registro distribuito che funge da database chiuso. A differenza del pubblico **Blockchain**, che sono "non autorizzati", **Blockchain private** sono "autorizzati" perché per diventare utente è necessaria l'autorizzazione. A differenza del pubblico **Blockchain**, che sono accessibili al pubblico a tutti, l'accesso ai **Blockchain private** dipende dall'autorizzazione a diventare un utente. Questa struttura permette di sfruttare la sicurezza e l'immutabilità dei **Tecnologia blockchain** pur rimanendo conformi alla protezione dei dati, in particolare rispettando le disposizioni del Regolamento generale sulla protezione dei dati (GDPR). I record blockchain privati possono essere modificati, modificati o eliminati. In questo contesto, per cancellazione si intende che il valore di riferimento per l'UUID (Universally Unique Identifier) nel provider**'s** il database viene eliminato. Inoltre, l'hash viene reso anonimo nel database blockchain, in modo che questo processo complessivo sia conforme al Regolamento generale sulla protezione dei dati e siano garantiti i diritti dell'interessato (diritto alla cancellazione "diritto all'oblio", art. 17 GDPR).

**Tipologia di dati memorizzati ed elaborati nella blockchain:**

- UUID del paziente
- Istituzioni/**Leistungserbinger** UUID
- UUID delle risorse
- Hash di **Compito di cura** e dati sulle risorse. (UUID: Universal Unique Identifier).

I dati memorizzati nel **Blockchain** è pseudonimizzato.
Nostro **Blockchain** è progettato per garantire la privacy in termini di integrità dei dati, profili dei pazienti, risorse e **Compiti di cura** e farmaci. Per comunicare con il **Blockchain**, l'utente deve registrare un insieme di chiavi pubbliche e private. Per comunicare con il **Blockchain**, l'utente necessita di diverse chiavi pubbliche e 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 memorizzata in forma crittografata nel **database del fornitore** , a cui può accedere solo il paziente.

In sede di verifica del consenso alla protezione dei dati, nel caso in cui il **provider** desidera comunicare con il paziente, il sistema verifica se il paziente ha accettato il **provider**. Le **Blockchain** Serve quindi a garantire l'integrità e la responsabilità del protocollo 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 c'è una comunicazione con il paziente, la blockchain risponde confrontando l'hash con un marcatore che indica se il consenso del paziente è ancora valido per l'attuale politica sulla privacy.
L'integrità del profilo del paziente è garantita anche dalla blockchain nella sincronizzazione del paziente. Le **Medico** Rileva immediatamente se il profilo del paziente non è sincronizzato o non corrisponde al profilo sul telefono cellulare confrontando l'hash del profilo del paziente sulla blockchain. In questo modo, il **fornitore di servizi raggiunge** sufficientemente aggiornati per quanto riguarda il profilo del paziente.

**Portale myoncare**:
Se il **fornitore di servizi** sceglie la soluzione blockchain, ONCARE implementa uno strumento aggiuntivo, chiamato "Adapter Service", che viene utilizzato per comunicare con il **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.

**Giustificazione del trattamento:** Il trattamento dei dati da parte di ONCARE per conto del **fornitore di servizi** viene effettuato sulla base dell'art. 28 GDPR (accordo sul trattamento dei dati).

**6. ELABORAZIONE DATI OPERATIVI**

Nel caso in cui l'utente sia una persona di contatto per il funzionamento del Portale presso la propria sede/studio (ad es. amministratore IT, professionista medico nominato), può fornirci alcuni dati personali quando ci contatta per comprendere o discutere le funzioni e l'utilizzo del Portale, o in caso di richiesta di servizio.

In caso di richiesta di assistenza, i seguenti dati personali possono essere visualizzati anche dai dipendenti autorizzati ONCARE:
I tuoi dati personali che ci hai fornito per la registrazione e/o l'accesso al nostro portale (ad es. nome, data di nascita, immagine del profilo, dati di contatto).
I dipendenti autorizzati di ONCARE che sono autorizzati ad accedere al database dell'utente allo scopo di elaborare 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 fornito da 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 il **Applicazione myoncare** per informarti su attività, scadenze 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 assicurerai di non perdere nessuna notifica importante e di garantire che il tuo supporto funzioni senza intoppi.

**Perché lo facciamo:**
Il nostro obiettivo è garantire che tu sia sempre informato sui tuoi compiti e aggiornamenti importanti al fine di supportare in modo ottimale la tua cura. 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 desideri ricevere notifiche push, puoi disattivarle nelle impostazioni dell'app myoncare.
- Assicurati che il tuo indirizzo e-mail sia accurato e aggiornato per garantire una ricezione regolare dei nostri messaggi.
- Se non desideri ricevere promemoria via e-mail, puoi disattivarli nelle impostazioni dell'app myoncare.

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:** indirizzo e-mail, data di nascita, data di registrazione, indirizzo IP, pseudo-chiavi generate dal portale.

L'app utilizza l'API di Google Maps per utilizzare le informazioni geografiche. Quando si usa Google Maps, Google raccoglie, tratta e utilizza anche i dati sull'uso delle funzioni della mappa. Ulteriori informazioni 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 del **Portale myoncare** e per contattarvi se necessario o direttamente da voi avviato (ad es. in caso di modifiche ai termini e alle condizioni, supporto necessario, problemi tecnici, ecc.). Inoltre, i dati personali (indirizzo e-mail) vengono elaborati nell'ambito dell'autenticazione a due fattori ogni volta che si accede al **Portale myoncare** .

**Giustificazione del trattamento:** Il trattamento dei dati aziendali è giustificato sulla base dell'art. 6 (1) (b) GDPR per l'esecuzione del contratto stipulato con ONCARE ai fini dell'utilizzo del **Portale myoncare** .

## 7. 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. Li utilizziamo per proteggere le nostre applicazioni e 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 altre informazioni 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 per il quale sono stati raccolti non sussiste più e non sussiste più un obbligo legale di conservazione. Per ulteriori informazioni sulle loro politiche sulla privacy, consultare https://ipapi.com/privacy/ e Informativa sulla privacy |Piattaforma di localizzazione Geoapify.

## 8. TRATTAMENTO DEI DATI (TRATTAMENTO)

Durante l'utilizzo del **Portale myoncare**, inserisci i dati personali (relativi alla salute) dei tuoi pazienti nel **Portale myoncare** (ad es. predisposizione di un piano di trattamento individuale, promemoria per l'assunzione di farmaci, ecc.). Inoltre, tu e i tuoi pazienti potete caricare documenti e file sul **Portale myoncare** e condividerli tra di noi. Inoltre, le funzioni di localizzazione possono essere generate e implementate:

- Aggiunta di una posizione;
- Caricamento del logo del sito web;
- Aggiungendo i dettagli della posizione;
- Caricare un'informativa sulla privacy;

E' possibile creare ulteriori requisiti di consenso per il paziente, per i quali il paziente deve fornire il consenso al fine di collegarsi al sito web.
Un'informativa sulla privacy caricata verrà mostrata a ogni paziente che si connette al sito web. Tutte le dichiarazioni di consenso devono essere documentate nell'informativa sulla privacy caricata. Una volta caricata, l'informativa sulla privacy può essere sostituita solo da una nuova versione, ma non può essere eliminata.
I file sono archiviati in un database cloud in Germania. È possibile consentire la condivisione di tali file con altri **Utenti del portale** all'interno della tua istituzione per scopi medici. Altri **utenti del portale** non hanno accesso a questi file.
È inoltre possibile consultare un fornitore di servizi esterno al proprio istituto (medico consulente) nel contesto del trattamento dei pazienti, se si ritiene che il parere di un altro esperto sia utile per il trattamento.

**In conformità con il GDPR, in qualità di titolare del trattamento dei dati, sei responsabile del trattamento dei dati sanitari dei pazienti nel contesto dell'utilizzo dei servizi myoncare.**

Trattiamo questi dati personali, compresi i dati sanitari del paziente, in base a un accordo con l'utente e in conformità con le sue istruzioni. Si prega di trattare i dati dei propri pazienti solo se si è ottenuto il consenso necessario ai dati da parte di questi pazienti. ONCARE agisce in qualità di responsabile del trattamento in conformità con l'accordo separato sul trattamento dei dati che abbiamo stipulato con l'utente sulla base dell'art. 28 GDPR.

## 9. TRATTAMENTO DEI DATI TECNICI DI UTILIZZO E DI SISTEMA

**Si applica solo se si utilizza myonclinic Store come utente del piano di cura.**

Le **Negozio Myonclinic** è integrato nel **Portale myoncare** e offre l'acquisto di piani di trattamento (Careplan). Dopo essersi registrati nel **Portale myoncare**, è possibile connettersi al **Negozio Myonclinic** con i tuoi dati di accesso. È possibile utilizzare il pulsante **Negozio Myonclinic** per acquistare piani di trattamento come utente.
**Dati dell'utente Careplan:**

I dati del **Utente Careplan**, che il **Negozio myonclinic** processi durante l'utilizzo, viene elaborato allo scopo di concludere un contratto di licenza con il **Fornitore di Careplan** – in questo caso ONCARE – e, se è dovuto un corrispettivo, per l'elaborazione e il controllo del processo di pagamento tra i **Fornitore di Careplan** – in questo caso ONCARE – e il **Utente Careplan** .

**Tipi di dati**: nome, dati di contatto, coordinate bancarie.

**Trattamento dei dati del negozio commerciale:** Dati personali da noi trattati durante l'utilizzo del **Negozio Myonclinic** nell'ambito dell'acquisto di piani di trattamento. Inoltre, i dati di pagamento (se viene addebitato un costo di utilizzo) saranno **inoltrato al fornitore del Careplan** .

**Giustificazione del trattamento dei dati del negozio commerciale:** La base giuridica per il trattamento dei dati dei negozi commerciali è l'art. 6 (1) (b) GDPR – il trattamento dei dati serve all'esecuzione del contratto tra **l'utente Careplan** e **il fornitore del Careplan** – in questo caso ONCARE.

## 10. TRATTAMENTO DEI DATI SULL'ATTIVITÀ

**Applicabile solo se gli utenti dell'app connessa acconsentono e abilitano il trasferimento dei dati.**

Le **Strumenti MyonCare** offerta **Utenti dell'app** la possibilità di collegare il **Applicazione myoncare** a determinate app per la salute (ad es. AppleHealth, GoogleFit, Withings) ("**App per la salute**"), a condizione che siano utilizzati dal **Utente dell'app** e la connessione è stabilita dal **Utente dell'app**. Una volta connessi, i dati dell'attività raccolti dal **App per la salute** saranno messe a disposizione dell'utente per fornire ulteriori informazioni contestuali in merito al **Utente dell'app**. Si prega di notare che i dati dell'attività **non ha origine** dagli strumenti myoncare e pertanto non deve essere utilizzato a fini diagnostici come base per decisioni mediche.

Il trattamento dei dati relativi all'attività è responsabilità dei pazienti.

**Tipi di dati:** Il tipo e l'entità dei dati trasferiti dipendono dalla decisione del **Utenti dell'app** . I dati includono, 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: il** Utente dell'app'**s Dati sull'attività** ti viene fornito al fine di fornire ulteriori informazioni contestuali relative al **Dell'utente dell'app** attività. Si prega di notare che i dati dell'attività non sono convalidati da **Gli strumenti MyonCare** e non deve essere utilizzato a fini diagnostici o come base per decisioni mediche.

**Motivo del trattamento:**
Il titolare del trattamento è il paziente stesso, che ti dà accesso ai dati della sua attività al fine di verificare le informazioni condivise. Non c'è quindi bisogno di ulteriori giustificazioni.

## 11. TRATTAMENTO DEI DATI SULLA SICUREZZA DEL PRODOTTO

**Si applica solo se si utilizza la variante per dispositivi medici degli strumenti myoncare.**

Le **Portale myoncare** E la **Applicazione myoncare** sono classificati e commercializzati come dispositivi medici in conformità con le normative europee sui dispositivi medici. In qualità di produttore di **Gli strumenti MyonCare**, dobbiamo rispettare determinati obblighi legali (ad es. monitoraggio della funzionalità dello strumento, valutazione delle segnalazioni di incidenti che possono essere correlate all'uso dello strumento, monitoraggio degli utenti, ecc.). Inoltre **Gli strumenti MyonCare** consentire all'utente di raccogliere dati personali su specifici dispositivi medici o farmaci utilizzati nel trattamento dei propri pazienti. I fabbricanti di tali dispositivi medici o medicinali hanno anche obblighi legali per quanto riguarda la sorveglianza del mercato (ad es. raccolta e valutazione delle segnalazioni di effetti collaterali).

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

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

**Elaborazione dei dati di 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 (per quanto possibile dopo la pseudonimizzazione) alle autorità competenti, agli organismi notificati o ad altri titolari del trattamento con obblighi di supervisione. Inoltre, conserviamo e trasferiamo i dati personali relativi ai dispositivi medici e/o ai medicinali quando riceviamo comunicazioni da parte dell'utente in qualità di segnalatore di tali informazioni, dal suo paziente o da terzi (ad es. i nostri distributori o importatori del **Strumenti MyonCare** nel proprio paese) che devono essere segnalati al produttore del prodotto affinché rispetti i propri obblighi legali in materia di sicurezza del prodotto.

**Motivazione 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 (1) (c), Art. 9 (2) (i) GDPR in combinato disposto con gli obblighi di monitoraggio post-commercializzazione 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.

**Integrazione dell'esclusione di responsabilità per effetti collaterali:**
Oncare GmbH non effettua alcuna valutazione medica dei contenuti trasmessi e non è obbligata a trasmettere alle autorità informazioni rilevanti per la legge farmaceutica come effetti collaterali, errori di applicazione o difetti del prodotto. Questa responsabilità spetta esclusivamente ai fornitori di servizi che trattano il trattamento o, se interessati, ai rispettivi produttori dei prodotti utilizzati.

**12. ELABORAZIONE DA PARTE DI PRODUTTORI DI APPARECCHIATURE E FORNITORI DI SERVIZI DI LABORATORIO**

Se l'utente utilizza funzioni mediche aggiuntive come la diagnostica integrata, la raccolta dei segni vitali o i servizi di laboratorio tramite la Piattaforma, i dati sanitari personali possono essere raccolti e trattati da terzi esterni (ad es. produttori di dispositivi medici o fornitori di servizi di laboratorio). Ciò avviene a supporto delle cure mediche e sempre sulla base di un consenso esplicito o di una relazione di trattamento.
Il trattamento viene effettuato nell'ambito dell'elaborazione degli ordini o, a seconda del fornitore, sotto la propria responsabilità ai sensi della legge sulla protezione dei dati. Oncare GmbH fornisce solo il collegamento tecnico a questo scopo, senza controllare o valutare il contenuto dal punto di vista medico. Ulteriori informazioni sul rispettivo trattamento dei dati possono essere ottenute direttamente dal fornitore di servizi di trattamento o tramite le informazioni sulla protezione dei dati dei fornitori terzi integrati.

**13. GESTIONE DEI DATI E DEI PERCORSI DEI NEGOZI COMMERCIALI**

Il portale myoncare offre ai fornitori di prestazioni registrati (ad es. medici) la possibilità di offrire e configurare percorsi di cura digitali tramite una funzionalità del webshop (ad es. in collaborazione con myon.clinic) e di assegnare i pazienti individualmente.
Nell'ambito dell'utilizzo di questa funzionalità, vengono trattati dati personali, in particolare dati sanitari, come informazioni sull'indicazione, durata raccomandata del trattamento o assegnazione del percorso. Questo trattamento dei dati serve all'individualizzazione e all'assegnazione di contenuti medici e viene effettuato sulla base dell'art. 6 (1) (b) e l'art. 9 (2) (h) GDPR.

Oncare fornisce l'infrastruttura tecnica e tratta i dati in questione in qualità di titolare del trattamento ai sensi dell'art. 4 n. 7 GDPR, nella misura in cui il trattamento è necessario per la fornitura delle funzioni della piattaforma. Tuttavia, la selezione dei contenuti e la progettazione medica dei percorsi sono di esclusiva responsabilità del rispettivo fornitore di servizi.
Nella misura in cui la fatturazione o la trasmissione dei dati vengono effettuate a terzi (ad es. uffici di fatturazione o partner della piattaforma come myon.clinic), tale trattamento avviene solo sulla base di accordi o disposizioni di legge corrispondenti.

**12. TRATTAMENTO DEI DATI DI RIMBORSO IN CASO DI TRASMISSIONE DI OGGETTI DI COSTO**

**(Applicabile solo se si utilizzano gli strumenti myoncare per il rimborso.)**
Le **Portale myoncare** vi supporta nell'avvio delle vostre procedure standard per il rimborso dei servizi sanitari che avete fornito ai vostri pazienti tramite il **Applicazione myoncare**. Per consentire la procedura di rimborso, il **Portale myoncare** supporta la raccolta dei dati personali (sanitari) dei vostri pazienti dal **Portale myoncare** al fine di facilitare la trasmissione di questi dati ai pagatori del paziente nell'ambito delle procedure di rimborso standard (l'Associazione dei medici di assicurazione sanitaria obbligatoria e/o la compagnia di assicurazione sanitaria del paziente). L'utente è il titolare del trattamento dei dati di rimborso ed è responsabile del rispetto delle norme sulla protezione dei dati per il trattamento dei dati personali dei suoi pazienti nel processo di rimborso. ONCARE agisce in qualità di Responsabile del trattamento dei dati sulla base dell'Accordo sul trattamento dei dati con il **Fornitore di servizi**.

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

**Trattamento dei dati di rimborso**: In qualità di titolare del trattamento, trasmetti i dati del trattamento del paziente necessari per il rimborso al pagatore (la tua compagnia di assicurazione sanitaria e/o la compagnia di assicurazione sanitaria del paziente) e il pagatore elabora i dati di rimborso al fine di rimborsarti.

**Motivo del trattamento dei dati di rimborso:** Il trattamento dei dati di rimborso viene effettuato sulla base dei §§ 295, 301 SGB V. Il trattamento dei dati da parte di ONCARE per Lei avviene anche sulla base dell'art. 28 GDPR (accordo di elaborazione degli ordini).

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

Le **Portale myoncare** funziona come uno strumento basato sul web per il quale è necessaria una connessione Internet funzionante e una 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 sulle 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;
- Preparazione e invio di un rapporto;
- Sostituisci le notifiche push con le email per **PWA** (Progressive Web App) nei seguenti casi:
  - → Se un piano di assistenza termina entro un giorno;
  - → se è stato assegnato un farmaco;
  - → se l'Informativa sulla privacy è stata aggiornata;
  - → quando un appuntamento viene inviato a pazienti e medici, in particolare per il tipo di appuntamento "videochiamata";
  - → Qualsiasi informazione relativa a un **di curadi compito** o se un **provider** ha assegnato un compito di cura.

**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.

**Brevo (Informativa sulla privacy):**
Informativa sulla privacy - Protezione dei dati personali | Brevo

**SendGrid**
SendGrid

**Matomo**
Questo è uno strumento di analisi web open source. Matomo (fornito da InnoCraft Ltd., Nuova Zelanda) non trasmette dati a server che sono al di fuori del controllo di ONCARE. Matomo è inizialmente disabilitato quando si utilizzano i nostri servizi. Solo se l'utente è d'accordo, il suo comportamento utente verrà registrato in forma anonima. Se questa opzione è disabilitata, 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:
- Sistema operativo dell'utente;
- Geolocalizzazione dell'utente;
-Browser;
-Ruolo;
-Indirizzo IP;
- Siti web visitati tramite il Web/PWA (per ulteriori informazioni, consultare la sezione relativa alle PWA nella presente Informativa sulla privacy);
- Pulsanti su cui l'utente fa clic nel file **Portale myoncare**Nel **Applicazione myoncare** e nel **myoncare PWA**.
Le informazioni generate dal cookie non saranno condivise con terze parti.

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, visitare: 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 degli utenti. 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.

## 14. 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 il portale, nonché da e verso l'app è crittografato. Offriamo SSL come protocollo di crittografia per la trasmissione sicura dei dati. Anche lo scambio di dati è crittografato e viene effettuato con pseudo-chiavi.

## 15. TRASFERIMENTI DI DATI/DIVULGAZIONE A TERZE PARTI

I vostri dati personali saranno trasmessi 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 è crittografata durante il transito.

Le informazioni su come gestiamo i dati personali (sanitari) dei vostri pazienti che utilizzano il **Applicazione myoncare** è riassunto in un **Informativa sulla privacy** per il **App per i pazienti Myoncare**. Puoi trovare il **Informativa sulla privacy per i pazienti** qui. Si prega di leggere attentamente anche la presente informativa sulla privacy per i pazienti. L'utente è il titolare del trattamento di una parte del trattamento dei dati dei pazienti ed è responsabile del rispetto della protezione dei dati (ad es. trasmissione dei dati di trattamento al paziente).

## 16. 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 dare il vostro consenso, vi informeremo sullo scopo del trattamento dei dati e sul vostro diritto di opposizione.
Se il consenso riguarda anche il trattamento di categorie particolari di dati personali, il **Portale myoncare** vi informerà espressamente di ciò nell'ambito della procedura di consenso.
Trattamento di categorie particolari di dati personali ai sensi dell'art. 9 (1) GDPR può avvenire solo se ciò è necessario a causa di disposizioni di legge e non vi è motivo di presumere che i tuoi legittimi interessi si oppongano al trattamento di questi dati personali o che tu abbia dato il tuo consenso al trattamento di questi dati personali ai sensi dell'art. 9 (2) GDPR.
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 **Portale myoncare** . Inoltre, ONCARE chiederà all'utente di accettare un accordo sul trattamento dei dati per i dati trattati da ONCARE sotto la sua responsabilità in qualità di titolare del trattamento.

## 17. DESTINATARI DEI DATI/CATEGORIE DI DESTINATARI

Nella nostra organizzazione, ci assicuriamo che solo le persone che sono obbligate a farlo per adempiere ai loro obblighi contrattuali e legali siano autorizzate al trattamento dei dati personali.

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 cloud storage e fornitori di servizi di supporto.
Google Firebase è un "database NoSQL" che consente la sincronizzazione tra il portale myoncare del tuo fornitore di servizi e l'app 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, è stata creata una pseudochiave del **Portale myoncare** E la **Applicazione myoncare** viene memorizzato in Google Firebase insieme al piano di trattamento 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 in transito e utilizzando pseudo-chiavi invece di identificatori personali come nomi o indirizzi e-mail per tracciare questi trasferimenti. La re-identificazione avviene non appena i dati personali hanno raggiunto l'account del paziente nel **Applicazione myoncare** o il tuo account nella sezione **Portale myoncare** previa verifica da parte di token specifici.

I nostri provider di archiviazione cloud offrono l'archiviazione cloud, che memorizza il gestore Firebase che gestisce gli URL Firebase per il **Portale myoncare**. Inoltre, questi fornitori di servizi forniscono il dominio server isolato del **Portale myoncare**, dove vengono conservati sia i tuoi dati personali che quelli dei tuoi pazienti. Ospita anche il servizio di gestione video e file di myoncare, che consente videoconferenze crittografate e condivisione dei dati tra te e il tuo paziente. L'accesso ai tuoi dati personali da parte tua e del tuo paziente è garantito dall'invio di token specifici. Questi dati personali sono crittografati durante la trasmissione e pseudonimizzati per ONCARE e i suoi fornitori di servizi durante la trasmissione e a riposo. I fornitori di servizi di 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 l'indirizzo e-mail salvato, 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 assistenza, ti verrà assegnato un numero di biglietto.
Se si tratta di una richiesta di servizio relativa all'utilizzo dell'account, le informazioni pertinenti fornite dall'utente al momento del contatto verranno inoltrate a uno dei dipendenti autorizzati del servizio esterno. Ti contatterà 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. Si tratta di una piattaforma di customer experience per la gestione dei feedback esterni con la capacità per creare ticket di supporto. Qui troverai il
Informativa sulla privacy: https://app.repaircode.de/?main=main-client – Legale/privacy.

Infine, ti mostriamo i contenuti di Instagram (fornitore: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublino 2, Irlanda) (ad es. immagini, video o post). Quando fai clic su un post di Instagram collegato, verrai reindirizzato a Instagram. Instagram può impostare i cookie ed elaborare i dati degli utenti.

Quando visiti una pagina con un post di Instagram collegato, il tuo browser può connettersi automaticamente 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 può assegnare la visita al tuo account utente.
Informativa sulla privacy: https://privacycenter.instagram.com/policy

**18. TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI**

Per fornire i nostri servizi, possiamo utilizzare fornitori di servizi che si trovano al di fuori dell'Unione Europea. Se i dati vengono trasferiti in un paese terzo in cui la protezione dei dati personali non è stata giudicata adeguata, ci assicureremo che siano adottate misure adeguate in conformità con il diritto nazionale ed europeo e, se necessario, che siano state concordate tra le parti del trattamento clausole contrattuali standard appropriate.

Dati personali raccolti dal **portale myoncare** o dall' **applicazione myoncare** non sono memorizzato negli app store. Il trasferimento di dati personali verso paesi terzi (al di fuori dell'Unione Europea o dello Spazio Economico Europeo) avviene 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 **Portale myoncare** colla **Applicazione myoncare** viene eseguito con l'aiuto di Google Firebase. I server di Google Firebase sono ospitati nell'Unione Europea. Tuttavia, secondo i termini e le condizioni generali di Google Firebase, un trasferimento temporaneo di dati nei paesi in cui Google e i relativi fornitori di servizi hanno filiali. Per alcuni servizi di Google Firebase, i dati vengono trasferiti solo negli Stati Uniti, a meno che il trattamento non avvenga nell'Unione Europea o nello Spazio Economico Europeo. L'accesso non autorizzato ai dati dell'utente viene impedito dalla crittografia end-to-end e da token per l'accesso sicuro. I nostri server online 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.

**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.

Incorporiamo i contenuti di Instagram forniti da Meta Platforms Ireland Ltd. Se l'utente clicca su un post di Instagram collegato, i dati personali (ad es. indirizzo IP, informazioni sul browser, interazioni) possono essere 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 a 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, ma la loro efficacia non può sempre essere garantita.

Per elaborare i dati dell'attività, sul dispositivo mobile dell'utente dell'app vengono utilizzate interfacce con i servizi Google Cloud (nel caso di GoogleFit) o con AppleHealth o Withings. Le **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 da **Gli strumenti MyonCare** non contiene dati personali. I dati personali sono messi a disposizione di **Strumenti MyonCare** tramite queste interfacce.

**19. DURATA DELLA CONSERVAZIONE DEI DATI PERSONALI**

Conserveremo i tuoi dati personali per tutto il tempo necessario allo scopo per il quale sono 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 ai sensi del diritto commerciale o fiscale.

Si prega di notare che ONCARE è inoltre soggetta a obblighi di conservazione che sono contrattualmente concordati con l'utente sulla base di disposizioni di legge. Inoltre, a causa della classificazione e, se applicabile, dell'utilizzo del **portale myoncare** e dell' **applicazione myoncare** in quanto dispositivo medico, al portale si applicano determinati periodi di conservazione, che derivano dalla legge sui dispositivi medici. Salvo diversa conservazione, i dati personali vengono 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 una controversia e utilizziamo le prove entro i termini di prescrizione previsti dalla legge, che possono arrivare fino a 30 anni; Il termine di prescrizione ordinario è di tre anni.

**20. I TUOI DIRITTI IN QUALITÀ DI INTERESSATO**

Diversi dati personali sono necessari per l'istituzione, l'esecuzione e la risoluzione del rapporto contrattuale e l'adempimento dei relativi obblighi contrattuali e legali. Lo stesso vale per l'uso del nostro **portale myoncare** e le varie funzioni che offre.

In alcuni casi, i dati personali devono essere raccolti o resi disponibili in conformità con la legge. Si prega di notare che senza la fornitura di questi dati personali, non è possibile elaborare la richiesta o adempiere all'obbligo contrattuale sottostante.

**21. DECISIONI AUTOMATIZZATE NEI SINGOLI CASI**

Per prendere decisioni utilizziamo un'elaborazione totalmente automatizzata.

**22. 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 e sulle modalità di trattamento dei propri dati personali, 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 richiedere la cancellazione dei propri dati personali raccolti e trattati da noi senza ingiustificato ritardo. In questo caso, ti chiederemo di eliminare il **Portale myoncare** dal tuo computer. 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 che lo riguardano 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 far valere diritti 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 qualora trattiamo i suoi dati personali sulla base del suo consenso. Continueremo a fornire i nostri servizi anche se non dipendono dalla revoca del consenso.
Per esercitare questi diritti, si prega di contattarci all'indirizzo: privacy@myoncare.com. L'opposizione e la revoca del consenso devono essere presentate a privacy@myoncare.com in forma scritta .
Ti chiediamo di fornire una prova sufficiente della tua identità per garantire che i tuoi diritti siano protetti e che i tuoi dati personali siano condivisi solo con te e non con 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.

**23. RESPONSABILE DELLA PROTEZIONE DEI DATI**

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

**24. SOGGETTO A MODIFICHE ALLA PRESENTE 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 conformarsi ai requisiti di legge, per tenere conto degli sviluppi tecnici ed economici o **per rendere giustizia a** Gli interessi dell'app **o** utenti del portale.

Le modifiche sono possibili in qualsiasi momento e saranno notificate all'utente in modo appropriato ed entro un periodo di tempo ragionevole prima della loro data di entrata in vigore (ad esempio, pubblicando un documento **Informativa sulla privacy** al momento del login o fornendo un preavviso di modifiche sostanziali).

ONCARE GmbH Indirizzo postale: Balanstraße 71a, 81541 Monaco di Baviera, Germania

E | +49 (0) 89 4445 1156 E | privacy@myoncare.com

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

Se i contenuti o i servizi medici vengono ottenuti o offerti tramite il negozio integrato myonclinic, il contenuto e la responsabilità economica sono a carico di myon.clinic GmbH, una consociata di Oncare GmbH. In questo contesto, Oncare GmbH fornisce solo la piattaforma tecnica.
privacy@myon.clinic

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

A PARTIRE DA GIUGNO 2025

* * *

Quanto segue **sono norme supplementari sulla protezione dei dati per i fornitori di servizi** che agiscono in qualità di entità coperta **in** gli Stati Uniti d'America **nell'ambito di** un'attività conforme a HIPAA **o per conto di tale entità**:

La protezione delle informazioni sanitarie personali (PHI) ai sensi dell'HIPAA si applica solo se questi dati vengono elaborati nell'ambito degli Stati Uniti. sistema sanitario da parte di un cosiddetto ente coperto o di un socio in affari, indipendentemente dalla nazionalità o dalla residenza dell'interessato. L'unico fattore decisivo è che il trattamento rientri nell'ambito di applicazione dell'HIPAA.

## US Disposizioni supplementari sulla protezione dei dati per i fornitori di servizi negli Stati Uniti d'America (HIPAA)

**1. Ambito di applicazione**

Il presente Addendum HIPAA si applica a tutti i fornitori di servizi che elaborano, archiviano o condividono informazioni sanitarie protette (PHI) attraverso la piattaforma ONCARE, a condizione che tale trattamento sia in relazione a un appaltatore regolamentato HIPAA ("Entità coperta") o che ONCARE agisca in qualità di socio in affari.

**2. Ruoli e responsabilità**

ONCARE agisce in qualità di socio in affari ai sensi della norma sulla privacy HIPAA (45 CFR §160.103) e si impegna a rispettare tutte le normative HIPAA applicabili all'Entità coperta. Il rispettivo fornitore di servizi agisce:

- in qualità di membro della forza lavoro dell'ente coperto o
- in qualità di subappaltatore di ONCARE ai sensi del 45 CFR §160.103 e seguenti.

**3. Telaio di lavorazione**

L'utilizzo della piattaforma ONCARE da parte dei fornitori di servizi si basa solo sugli accordi esistenti conformi alla normativa HIPAA con l'entità interessata (ad es. accordi di società in affari o accordi con i fornitori di servizi). Il trattamento comprende in particolare:
- Documentazione dei corsi di trattamento e delle prestazioni mediche,
- Comunicazione con i pazienti utilizzando canali di comunicazione conformi a HIPAA (crittografia end-to-end, TLS)
- Accesso ai dati strutturati dei pazienti per l'assistenza o la garanzia della qualità.

**4. Riservatezza e controllo degli accessi**

I fornitori si impegnano a mantenere riservate tutte le PHI e a limitare l'accesso alle PHI nella misura necessaria in conformità con lo standard minimo necessario (45 CFR §164.502(b)). Ogni accesso è gestito tramite un concetto di diritti basato sui ruoli e registrato in modo verificabile.

**5. Misure di sicurezza tecniche e organizzative**

Tutte le misure di sicurezza implementate da ONCARE sono conformi ai requisiti della norma di sicurezza HIPAA (45 CFR Parte 164, Sottoparte C). Questi includono:

- crittografia AES-256 dei dati memorizzati,

- trasmissione crittografata tramite TLS 1.3,
- Autenticazione a due fattori (2FA),
- analisi periodiche dei rischi ai sensi del §164.308(a)(1)(ii)(A),
- processi strutturati di risposta agli incidenti.

**6. Trattamento dei dati al di fuori degli Stati Uniti**

Quando i Fornitori accedono ai dati tramite ONCARE che vengono elaborati o archiviati al di fuori degli Stati Uniti (ad esempio, l'hosting nell'UE), lo fanno esclusivamente:
- sulla base di una protezione contrattuale conforme alla normativa HIPAA (ad es. subappaltatore BAA),
- con il consenso documentato dell'Ente Coperto,
- in conformità con la norma di sicurezza HIPAA e gli standard internazionali complementari (es. B. ISO 27001, principi GDPR),
- e con crittografia end-to-end e controllo degli accessi.

**7. Obblighi di segnalazione in caso di incidenti relativi alla protezione dei dati**

I fornitori sono tenuti a notificare immediatamente a ONCARE qualsiasi incidente che possa portare all'accesso non autorizzato alle PHI ("Incidente di sicurezza" o "Violazione" come definito in 45 CFR §164.304/§164.402). ONCARE si occupa del coordinamento delle segnalazioni obbligatorie per legge all'ente coperto e alle persone interessate.

**8. Diritti dell'Ente Coperto**

L'Ente Coperto si riserva il diritto in qualsiasi momento di verificare l'accesso, l'uso e le misure di sicurezza relative alle PHI da parte di ONCARE e dei Fornitori di Servizi Associati. I fornitori di servizi devono garantire la piena collaborazione.

**9. Nessuna distribuzione indipendente**

Il Fornitore di servizi può divulgare le informazioni sanitarie protette a terzi al di fuori della Piattaforma (ad esempio, tramite e-mail, sistema esterno, stampa) solo se:

- vi sia una "autorizzazione" documentata da parte dell'interessato oppure
- Ciò è espressamente previsto nel contratto.

**10. Precedenza e interpretazione**

In caso di conflitto tra il presente Supplemento HIPAA e le norme europee sulla protezione dei dati, si applicherà sempre la norma più rigorosa, a condizione che sia coerente con la legge applicabile. Stati Uniti Le leggi federali sulla privacy (ad esempio, CCPA) rimangono inalterate e le leggi statali sulla privacy rimangono inalterate e si applicano in aggiunta, ove applicabile.

**11. Sostegno ai diritti degli interessati**

I fornitori di servizi supportano ONCARE e la rispettiva Entità coperta nell'adempimento dei diritti degli interessati ai sensi del 45 CFR §§ 164.524-528 (ad es. informazione, correzione, limitazione della divulgazione). Ciò include, in particolare, la partecipazione a:
- la fornitura di log di accesso ("Accounting of Disclosures"),
- la correzione di informazioni sanitarie protette errate,
- l'attuazione di avvisi di blocco o restrizioni d'uso.

Le richieste saranno coordinate da ONCARE ed evase con un preavviso di 30 giorni, con eventuale proroga di altri 30 giorni dalla comunicazione.

**12. Obbligo di formazione in materia di protezione dei dati**

I fornitori di servizi sono tenuti a condurre ogni anno un corso di formazione documentato sui requisiti di protezione dei dati secondo HIPAA e GDPR.
ONCARE fornisce materiali adeguati o l'accesso all'e-learning a questo scopo. La partecipazione è documentata digitalmente e deve essere dimostrata all'Ente Coperto su richiesta.

**13. Dati sull'uso secondario e sulla ricerca**

Qualsiasi utilizzo di PHI per scopi di ricerca, analisi o marketing da parte del Fornitore di servizi è vietato a meno che:
- esiste un consenso documentato ("Autorizzazione") ai sensi del 45 CFR §164.508,
- o è stato stipulato con ONCARE un accordo specifico sull'utilizzo dei dati di ricerca conforme alla normativa HIPAA.

L'uso secondario interno (ad es. per la garanzia della qualità) è consentito solo nell'ambito della limitazione dello scopo HIPAA.

**14. Coordinamento con i requisiti del GDPR**

Con l'applicabilità simultanea del GDPR e dell'HIPAA, ONCARE garantisce che si applichi sempre il livello di protezione più rigoroso. In particolare, i fornitori di servizi si impegnano a:

- non trasferire dati al di fuori del SEE senza adeguate clausole contrattuali standard o sub-BAA;
- Coordinare i diritti degli interessati di entrambe le giurisdizioni (ad esempio, il diritto alla cancellazione ai sensi dell'art. 17 GDPR vs. obblighi di conservazione ai sensi dell'HIPAA) in conformità con ONCARE.

**15. Requisiti statali supplementari in materia di protezione dei dati (USA)**

Oltre alle normative federali dell'Health Insurance Portability and Accountability Act (HIPAA), alcuni trattamenti dei dati sono soggetti a leggi supplementari o più severe sulla protezione dei dati dei singoli stati degli Stati Uniti. Ciò vale in particolare se gli utenti interessati risiedono in uno di questi stati, utilizzano i nostri servizi da lì o se i dati personali vengono elaborati da fornitori di servizi o partner contrattuali con sede in questi stati.

Le seguenti leggi federali sulla privacy possono essere applicate in aggiunta o in via prioritaria, a seconda della singola costellazione:
- California: California Consumer Privacy Act (CCPA) e California Privacy Rights Act (CPRA)
- New York: Legge sullo scudo
- Virginia: Legge sulla protezione dei dati dei consumatori della Virginia (VCDPA)
- Colorado: Legge sulla privacy del Colorado (CPA)
- Connecticut: Legge sulla privacy dei dati (CTDPA)
- Utah: Legge sulla privacy dei consumatori dello Utah (UCPA)
- Illinois: Legge sulla privacy delle informazioni biometriche (BIPA)
- Texas: Legge sulla privacy e la sicurezza dei dati (TDPSA, in vigore dal 01.07.2024)
- Florida: Carta dei diritti digitali (FDBR)

Ci impegniamo a rispettare le normative federali applicabili per tutte le attività di trattamento e a fornire agli interessati informazioni complete sull'applicazione di questi diritti su richiesta. Per alcuni stati (ad esempio, la California), forniamo informative sulla privacy separate su richiesta. Contattateci all'indirizzo **privacy@myoncare.com** se l'utente desidera esercitare i propri diritti in materia di privacy ai sensi della legge federale o statale.

**16. Nessun uso commerciale dei dati personali dell'utente del portale**
I dati personali degli utenti del portale (ad es. fornitori di servizi sanitari) non vengono utilizzati per scopi di ricerca, marketing o altri scopi commerciali. ONCARE elabora solo dati tecnici di utilizzo completamente anonimizzati (ad es. timestamp di accesso aggregati o modelli di utilizzo del sistema) per migliorare le prestazioni tecniche della piattaforma. Questi dati non contengono alcuna informazione che potrebbe essere utilizzata per identificare i singoli utenti e non sono considerati informazioni sanitarie protette (PHI) ai sensi della norma sulla privacy HIPAA.

***