Benvenuti su myoncare, il portale digitale per la salute e l'app mobile ("**App**") per un'assistenza efficiente e adeguata alle esigenze dei pazienti e un supporto per la gestione della salute sul lavoro.

La presente informativa sulla privacy è suddivisa in due parti:

- La prima parte contiene le norme sulla protezione dei dati per l'utilizzo della piattaforma myoncare in Europa in conformità con il **Regolamento generale sulla protezione dei dati (GDPR) dell'UE.**

- La seconda parte contiene **Informazioni aggiuntive** conformemente ai requisiti del **la legge sulla protezione dei dati degli Stati Uniti d'America (HIPAA),** in particolare per gli utenti residenti negli Stati Uniti o in caso di trattamento di dati sanitari da parte di fornitori di servizi sanitari statunitensi.

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 **App** è di grande importanza e 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. In questa informativa sulla privacy, scoprirai 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, avrai l'opportunità di accettare l'Informativa sulla privacy e acconsentire al trattamento dei tuoi 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.

1. DEFINIZIONI

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

"**Blockchain**" è un altro database 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 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.

"**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 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 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.

"**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.

"**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, 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 e utente dell'App myoncare, che descrive il modo in cui raccogliamo, utilizziamo e conserviamo le informazioni personali dell'utente e lo informa dei suoi ampi diritti.

"**Condizioni d'uso**" indica i termini di utilizzo per l'utilizzo dell'App 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 il **applicazione mobile myoncare App** e lo gestisce come accesso al **Servizi myoncare**. Questo **Informativa sulla privacy** si applica a tutti i dati personali trattati da ONCARE in relazione all'utilizzo del **Applicazione myoncare** .

3. 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 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, "**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.

4. 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.

5. 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 nel nostro **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 della 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 dal **Medico** , le attività pianificate e completate.

Dati del negozio commerciale: Dati del Negozio Commerciale: dati personali trattati in relazione all'utilizzo del Negozio myoncare, 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 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** 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.

Utilizzo di dati anonimizzati per scopi commerciali: Inoltre, ONCARE può utilizzare alcuni dati sanitari e di utilizzo, una volta completamente anonimizzati, per scopi commerciali, come il miglioramento della piattaforma, l'analisi dei processi di assistenza o lo sviluppo di nuovi servizi sanitari digitali. L'anonimizzazione avviene in modo tale che le persone non possano più essere identificate. Questi dati anonimizzati non sono quindi più soggetti al GDPR.

Dati provenienti da produttori di dispositivi, distributori di dispositivi medici o laboratori:
Inoltre, i dati personali possono essere trattati da produttori di dispositivi medici connessi, distributori di dispositivi medici o 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 dei prodotti: Dati personali trattati per adempiere ai nostri obblighi legali in qualità di produttore del **Applicazione myoncare** come dispositivo medico. Inoltre, i tuoi dati personali possono essere trattati da aziende di dispositivi medici o 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 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 sulla salute in generale.

6. TECNOLOGIA BLOCKCHAIN

Blockchain **Tecnologia** ("**Blockchain**") (brevetto europeo n. 4 002 787) è un servizio opzionale che non è obbligatorio. È il tuo **fornitore di servizi** chi 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 in cui sono memorizzati i dati dell'applicazione. Tutti i dati blockchain sono archiviati nella Repubblica Federale Tedesca. 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 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. 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. In questo caso, il blocco non può più essere sincronizzato con gli altri. Questo processo tecnico impedisce a persone non autorizzate di manipolare il contenuto del **Blockchain** catena. Quando tutti i nodi (nodi della rete) tentano di sincronizzare le proprie copie, rileva che una copia è stata modificata e la rete considera tale nodo non integro.

Nostro **Blockchain** è un privato **Blockchain**. Un privato **Blockchain** è decentralizzato. Si tratta di un cosiddetto sistema di registro distribuito che funge da database chiuso. A differenza del pubblico **Blockchain**, che sono "non autorizzati", privati **Blockchain** 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 servizi privati **Blockchain** dipende dall'idoneità a diventare un utente. Questa struttura consente di sfruttare la sicurezza e l'immutabilità della tecnologia blockchain nel rispetto della protezione dei dati e, in particolare, delle norme 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 il valore di riferimento all'UUID (Universally Unique Identifier) nel servizio **del fornitore** il database viene eliminato. Inoltre, l'hash è 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:

- Istituzioni/**Leistungserbinger** UUID
- UUID del paziente
- Asset UUID
- Hash dei dati delle attività di cura e degli asset. (UUID: Universal Unique Identifier).

I file memorizzati nel file **Blockchain** sono pseudo-anonimizzati.

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 il **Blockchain**, l'utente ha bisogno di diverse chiavi pubbliche-private; Il processo di registrazione genera certificati che vengono memorizzati in un database separato del **provider** e sul cellulare del paziente. Una copia di backup della chiave del paziente viene crittografata e memorizzata nel **provider**, a cui può accedere solo il paziente.

In sede di verifica del consenso alla protezione dei dati, nel caso in cui il **Provider** vuole comunicare con il Paziente, il sistema verifica se il Paziente ha dato il consenso alla Privacy Policy del Fornitore. Le **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 dato il consenso, tale interazione viene memorizzata sul **Blockchain** . Ogni volta che il paziente comunica, 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 . Le **Medico** 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, 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.

Base giuridica del trattamento dei dati: 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).

7. TRATTAMENTO DEI DATI OPERATIVI

Applicabile a tutti gli utenti dell'app

L'utente può fornirci alcuni dati personali quando ci contatta per comprendere le funzioni e l'uso del **Applicazione myoncare** , in caso di richiesta di assistenza da parte dell'utente o in caso di offerta di assistenza avviata da noi (telefonicamente).

Dipendenti del servizio
Per conto del titolare del trattamento dei dati (ad es. Vi offriamo supporto nella compilazione di questionari telefonici (chiamate in uscita) al fine di ottimizzare la vostra assistenza digitale al paziente. Se non si desidera usufruire di questa offerta, si è liberi di non accettarla e di opporsi all'assistenza telefonica.

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

- I dati personali che hai fornito al tuo **fornitore di servizi** tramite la nostra app (ad es. nome, data di nascita, immagine del profilo, dati di contatto).

- I dati sanitari che hai fornito al tuo **Medico** dati **fornitore di servizi** o **datore di lavoro** tramite il nostro **Applicazione myoncare** (ad es. informazioni sui farmaci assunti, risposte a questionari che includono informazioni relative a malattie o condizioni, diagnosi e terapie di operatori sanitari, compiti pianificati e completati).

Dipendenti ONCARE autorizzati che possono accedere al database del fornitore di servizi dell'utente**,** Fornitore di servizi dati **o** datore di lavoro **ai fini dell'elaborazione di una richiesta di servizio o 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 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 WebApp) e **L'app 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 aggiornato sulle tue attività e sugli aggiornamenti importanti per sostenere la tua salute nel miglior modo possibile.
- 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.

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.

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.

Quando l' **Applicazione myoncare** viene scaricata, le informazioni necessarie vengono trasmesse al fornitore dell'app store. Non abbiamo alcuna influenza 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 il nostro **App Myoncare** e servizi.

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. 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 **Applicazione myoncare** e di contattarvi direttamente, se necessario o avviato da voi (ad es. in caso di modifiche alle condizioni generali, supporto necessario, problemi tecnici, assistenza nella compilazione dei questionari, ecc.).

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 **Applicazione myoncare** .

8. 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, visitare il sito https://ipapi.com/privacy/

9. TRATTAMENTO DEI DATI

Applicabile agli utenti dell'app che utilizzano l'app con il proprio fornitore di servizi.

Durante l'utilizzo del **Applicazione myoncare**La tua **fornitore di servizi** può inserire i tuoi dati personali nella sezione **Portale myoncare** per avviare il **Servizi MyonCare** (ad es. creazione di te come paziente, fornitura di un compito individuale, promemoria per l'assunzione di farmaci, ecc.). Inoltre, tu e il tuo **il fornitore di servizi può caricare** documenti e fascicoli al **Applicazione myoncare** E la **Portale myoncare** e condividerli tra di noi. La tua **provider** può caricare un **Informativa sulla privacy** per tua informazione e impostare altri requisiti di consenso per te come paziente per i quali è richiesto il tuo consenso. I file sono archiviati in un database cloud in Germania. La tua **fornitore di servizi** consentire la condivisione di tali file con altri **Utenti del portale** all'interno della sua istituzione o di altri **Fornitori** al di fuori della propria struttura (medici consulenti) per scopi medici. Gli altri utenti del portale non avranno accesso a questi file senza questa condivisione. Inoltre, il tuo **fornitore di servizi** può incaricarci di assistervi telefonicamente nella compilazione di questionari (chiamate in uscita). Questa operazione viene eseguita solo secondo le istruzioni del fornitore di servizi e viene eseguita esclusivamente da dipendenti ONCARE autorizzati.

Utilizzeremo e tratteremo i tuoi dati in conformità con il **termini stabiliti nella presente Informativa sulla privacy**, a condizione che l'utente ci fornisca il suo consenso ove richiesto.

Trattiamo questi dati personali, compresi i dati sanitari dell'utente, in base a un accordo e in conformità con le istruzioni dell'utente **Medico**. Per queste finalità di trattamento, il **fornitore di servizi** è responsabile del trattamento dei dati personali e dei dati sanitari dell'utente in qualità di titolare del trattamento dei dati ai sensi delle leggi applicabili in materia di protezione 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 **fornitore di servizi**. In caso di domande o dubbi sul trattamento dei propri dati personali o sanitari, è necessario contattare in primo luogo il proprio medico curante.

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 con informazioni relative a malattie o condizioni, diagnosi e terapie da parte di operatori sanitari, attività pianificate e completate.

Finalità del trattamento dei dati: Trattiamo i vostri dati di trattamento al fine di fornire il nostro **Servizio MyonCare** al tuo **fornitore di servizi** e a te. I vostri dati sanitari, che inserite nel nostro **Applicazione myoncare** , verrà utilizzato dal tuo **fornitore di servizi** per consigli e supporto per te. Trattiamo questi dati personali in base a un accordo e in conformità con le istruzioni del vostro **fornitore di servizi**. 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 **Fornitori**.

Giustificazione del trattamento dei dati: I tuoi dati personali (trattamento) saranno trattati dal tuo **fornitore di servizi** 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 (2) (h) GDPR per i dati sanitari in quanto dati particolarmente sensibili, nonché il consenso dell'utente ai sensi dell'art. 6 (1) (a) e 9 (2) (a) GDPR. Il trattamento dei dati da parte di ONCARE per la propria **Fornitori** viene effettuato anche sulla base dell'art. 28 GDPR (Accordo sul trattamento dei dati).
La tua **fornitore di servizi** è responsabile dell'ottenimento del consenso dell'utente in qualità di titolare del trattamento dei dati. Anche se puoi usare il **Applicazione myoncare** Senza tale consenso, la maggior parte delle funzioni non funzionerà più (ad es. la condivisione dei dati con il proprio operatore sanitario). Il rifiuto o la revoca del consenso al trattamento dei dati comporta quindi una grave limitazione della funzionalità dei servizi dell'app e del tuo **Fornitori** non può più supportarti tramite il **Applicazione myoncare**.

10. 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**"). Al fine di consentire il trattamento dei dati relativi all'attività, otteniamo preventivamente il consenso dell'utente al trattamento. Se la connessione viene stabilita dopo il consenso dell'utente, il **dati sull'attività raccolti** dal **App per la salute** saranno messi a disposizione dei tuoi fornitori per 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 **Medico** a fini diagnostici come base per il processo decisionale medico. Si prega inoltre di notare che il vostro **Provider** non sono tenuti a verificare i dati della tua attività e non sono tenuti a fornirti un feedback sui dati della tua attività.
I dati dell'attività sono condivisi **con il tuo affiliato** fornitori di servizi ogni volta che il **Applicazione myoncare** è accessibile . Puoi revocare il tuo consenso alla divulgazione dei dati dell'attività in qualsiasi momento nelle impostazioni del **Applicazione myoncare**. Tieni presente che da questo momento in poi i dati della tua attività non saranno più condivisi. I dati dell'attività che sono già stati condivisi non verranno eliminati dal **Portale myoncare** dei tuoi affiliati **Fornitori**.

Il trattamento dei dati relativi alle attività è di competenza dell'utente.

Tipi di dati: Il tipo e la quantità di dati trasferiti dipendono dalla decisione dell'utente e dalla disponibilità di tali dati all'interno del **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: I tuoi Dati di Attività saranno forniti al tuo Affiliato **Provider** per fornire ulteriori informazioni contestuali sulla tua attività.

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

11. TRATTAMENTO DEI DATI SULLA SICUREZZA DEL PRODOTTO

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

Le **Applicazione myoncare** è classificato e commercializzato come dispositivo medico in conformità con il Regolamento Europeo sui Dispositivi Medici. In qualità di produttore dell'app, siamo tenuti a rispettare determinati obblighi legali (ad es. monitoraggio della funzionalità dell'app, valutazione dei rapporti sugli incidenti che potrebbero essere correlati all'utilizzo dell'app, tracciamento degli utenti, ecc.). Inoltre, il **Applicazione myoncare** permette a te e al tuo **Medico** per comunicare e raccogliere informazioni personali su specifici dispositivi medici o farmaci utilizzati nel trattamento. 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: Rapporti di casi, dati personali forniti in un rapporto 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 (per quanto possibile dopo la pseudonimizzazione) alle autorità competenti, agli organismi notificati o ad altri titolari del trattamento con compiti di vigilanza. Inoltre, conserviamo e trasferiamo i dati personali relativi a dispositivi medici e/o medicinali quando riceviamo comunicazioni dal vostro **Medico**, da voi come pazienti o da terzi (ad es. i nostri distributori o importatori **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.

Giustificazione del trattamento dei dati sulla sicurezza dei prodotti: La base giuridica per il trattamento dei dati personali per l'adempimento degli obblighi di legge in qualità di produttore di dispositivi medici o farmaci 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. TRATTAMENTO DEI DATI SANITARI E DI TRATTAMENTO

Applicabile agli utenti dell'app che utilizzano l'app con il proprio fornitore di servizi a scopo di rimborso.
Le **Applicazione myoncare** supporta il tuo **Medico** nell'avviare procedure standard per il rimborso dei servizi sanitari forniti all'utente tramite il **Applicazione myoncare**. Al fine di consentire la procedura di rimborso, il **Applicazione myoncare** supporta la raccolta dei tuoi dati personali (sanitari) da parte **fornitore di servizi** allo scopo di trasmettere questi dati all'ente pagante 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 **fornitore di servizi** 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 del **Fornitore di servizi**. Il tuo fornitore di servizi è il titolare del trattamento dei dati di rimborso. ONCARE agisce in qualità di responsabile del trattamento dei dati sulla base dell'accordo sul trattamento dei dati con l'utente **fornitore di servizi**.

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

Trattamento dei dati di rimborso: La tua **provider** trasmette i dati di trattamento necessari per il rimborso al pagatore (il suo ente di assicurazione sanitaria obbligatoria e/o la tua compagnia di assicurazione sanitaria) e il pagatore elabora i dati di rimborso al fine di fornire il rimborso al tuo **provider** .

Giustificazione del trattamento dei dati di rimborso: I dati di rimborso vengono elaborati sulla base dei §§ 295, 301 SGB V, art. 9 par. 2 lett. b GDPR. Trattamento dei dati da parte di ONCARE per **fornitore di servizi** viene effettuato anche sulla base dell'art. 28 GDPR (accordo di elaborazione degli ordini).

13. TRATTAMENTO DA PARTE DI PRODUTTORI DI DISPOSITIVI, DISTRIBUTORI DI DISPOSITIVI MEDICI 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 ed elaborati da fornitori terzi esterni (ad es. produttori di dispositivi medici, distributori di tali 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.

14. 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.

15. TRATTAMENTO DEI DATI RELATIVI ALLA GESTIONE DELLA SALUTE IN AZIENDA

Applicabile agli utenti dell'app che utilizzano l'app con il sistema di gestione della salute sul lavoro dell'azienda.

Durante l'uso del **Applicazione myoncare** in **la gestione della salute in azienda**, alcuni dati personali (sanitari) sono trasmessi in forma aggregata come dati per la gestione della salute sul lavoro **società** E la **Fornitori di dati** Commissionato **dall'azienda** (ad es. analisti di dati o società di ricerca). Né il **Società** né alcun **Fornitore di servizi dati** può associare tali dati alla tua identità. ONCARE consiglia **che non condividi alcun dato personale** Durante l'utilizzo dei servizi myoncare nell'ambito della gestione della salute sul lavoro.

Ciò significa che ONCARE e tutti i **I fornitori di dati** Elaborare i dati per la gestione della salute in azienda solo in conformità con l'azienda**'s** disposizioni. Trattiamo tali dati per la gestione della salute sul lavoro, compresi i vostri dati sanitari, sulla base di un accordo con il vostro **società** e/o un **Fornitore di dati** e in conformità con le loro istruzioni. Ai fini del presente accordo, il **Società** o il **Fornitore di dati** è il titolare del trattamento dei dati dell'utente per finalità di gestione della salute sul lavoro, nonché ONCARE e qualsiasi **Fornitori di dati** ingaggiato dal **Società** 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 **.**

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 potervi offrire **società** nostro **Servizi MyonCare**. I vostri dati di gestione della salute in azienda, che inserite nel nostro **Applicazione myoncare**, sarà utilizzato dal **società** (direttamente o tramite un **Fornitore di dati**) nell'ambito della 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 del **società** e/o un **Fornitore di 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 il **Società**.

Giustificazione del trattamento dei dati relativi alla gestione della salute sul lavoro: I vostri dati di gestione della salute in azienda saranno trattati dal **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 (1) (a) e l'art. 9 (2) (a) del GDPR o di un'altra base giuridica applicabile al **Società**. Il trattamento dei dati da parte di ONCARE per conto del **Società** (direttamente o tramite un fornitore di servizi incaricato dalla Vostra Società) si basa anche sull'art. 28 GDPR (Accordo sul trattamento dei dati).
Le **Società** , in qualità di titolare del trattamento, è responsabile dell'ottenimento del consenso dell'utente ove richiesto dalle normative 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.

16. 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 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 tra un'ora;
  - → 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.

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 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:

- Ruolo;
- geolocalizzazione dell'utente;
- Sistema operativo dell'utente;
- tempo in cui l'utente ha utilizzato il contenuto;
- -Indirizzo IP;
- Siti web visitati via web/ **PWA** (per ulteriori informazioni, consultare la sezione relativa alle PWA nella presente Informativa sulla privacy);
- Pulsanti che l'utente **fa clic su nella finestra di dialogo** Portale myoncare**Le** Applicazione myoncare **E la** 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 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.

17. 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 la trasmissione sicura dei dati. Anche lo scambio di dati è crittografato e viene effettuato con pseudo-chiavi.

18. 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 è crittografata durante il transito.

19. 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 si riferisce anche al trattamento di categorie particolari di dati personali, l'app myoncare informerà espressamente l'utente 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 richiesto dalla legge e non vi è motivo di ritenere che i tuoi interessi legittimi 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 (2) 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 la registrazione, i consensi possono essere gestiti nelle impostazioni dell'account dell'app myoncare.
La revoca del consenso è efficace solo per il futuro. Il trattamento effettuato fino al momento della revoca resta lecito (art. 7 par. 3 GDPR).

20. 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 sanitari che inserisci nel nostro **Applicazione myoncare** sarà messo a disposizione del vostro **Medico** e/o il tuo **società**, direttamente o tramite un **Fornitore di dati** (a seconda del tipo di utilizzo del **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 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 la **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, è stata creata una pseudochiave del **L'app myoncare è memorizzata in Google Firebase** insieme al corrispondente **piano di medicazione**. 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 tra l'utente e il suo **fornitore di servizi** o **società** (direttamente o a un **Fornitore di dati**) e utilizzando pseudochiavi invece di identificatori personali come nome o indirizzo e-mail per tenere traccia di questi trasferimenti. La re-identificazione avviene non appena i dati personali hanno raggiunto l'account del tuo **fornitore di servizi** o società nel **Portale myoncare** o il tuo account nella sezione **Applicazione myoncare**, dopo che è stato verificato da token speciali.

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 sono conservati i tuoi dati personali. Ospita anche i servizi di gestione video e file di myoncare, che consentono videoconferenze crittografate tra l'utente e il suo **fornitore di servizi**, così come la condivisione di file. Accesso ai tuoi dati personali da parte tua e dei tuoi **fornitore di servizi** è garantito dall'invio di token specifici. Questi dati personali sono crittografati in transito e a riposo e pseudonimizzati per ONCARE e i suoi fornitori di servizi. 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 di elaborare le 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, 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, 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 post di Instagram collegati, 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

21. 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.
I dati personali raccolti dall' **applicazione myoncare** non sono memorizzati 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 **Applicazione myoncare** E la **Portale myoncare** viene fatto tramite Google Firebase. Il server di Google Firebase è ospitato nell'Unione Europea. Tuttavia, come descritto nei Termini di servizio di Google Firebase, i trasferimenti di dati a breve termine possono essere effettuati nei 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 il trattamento 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 e per i clienti statunitensi negli Stati Uniti. 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.

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.

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. Inoltre, sono state implementate ulteriori misure tecniche di protezione, come la crittografia end-to-end e una rigorosa limitazione dell'accesso tramite token basati sui ruoli. Ciò serve a garantire ulteriormente il trasferimento dei dati ai sensi della sentenza "Schrems II" della Corte di giustizia.

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. **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 dal **Strumenti MyonCare** non contiene dati personali. I dati personali sono messi a disposizione di **Strumenti MyonCare** tramite queste interfacce.

22. 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, ma non esclusivamente, per gli obblighi di ritenzione ai sensi del 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 il **fornitore di servizi** sulla base di disposizioni di legge. Inoltre, e solo se il tuo **Il fornitore di servizi utilizza** la variante del dispositivo medico del **Strumenti MyonCare**, si applicano determinati periodi di conservazione derivanti dalla legge sui dispositivi medici a causa della classificazione dei **Applicazione myoncare** come dispositivo medico. 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.

23. OBBLIGO DI FORNIRE I DATI PERSONALI
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'utilizzo della nostra app myoncare e delle varie funzioni che offre.

Abbiamo riassunto i dettagli per te nei punti sopra menzionati. 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.

24. DIRITTI DI 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 il **Applicazione myoncare** Per funzionare sul tuo dispositivo, all'app devono essere concesse varie autorizzazioni per accedere a determinate funzionalità del dispositivo. Se necessario, li elencheremo in ordine di sistema operativo (Android o iOS) secondo il "Framework".
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 di 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.

Disabilitazione della 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 tramite dati mobili.

Accesso alla fotocamera
L'accesso alla fotocamera è necessario sia per la scansione del codice QR che 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 connesso.

Utilizziamo le notifiche push, che sono messaggi che vengono inviati al tuo dispositivo mobile come servizio del **Applicazione myoncare** attraverso servizi come l'Apple Push Notification Service o il 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.

25. DECISIONI AUTOMATIZZATE CASO PER CASO

Per prendere decisioni utilizziamo un'elaborazione totalmente automatizzata.

26. 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 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 richiedere la cancellazione dei propri dati personali raccolti e trattati da noi senza ingiustificato ritardo. In questo caso, ti chiederemo di eliminare il **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 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. Una revoca è efficace solo per il futuro. Il trattamento effettuato fino al momento della revoca rimane lecito.

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

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.

27. 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.

28. LIMITE DI ETÀ PER LA PRESENTAZIONE DELLA DOMANDA

Per utilizzare il **Applicazione myoncare** .

29. 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 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 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 è vincolante e autorevole.

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

Per le transazioni nel negozio myoncare, in particolare in relazione ai piani di trattamento (percorsi), la responsabilità economica e relativa ai contenuti è di myon.clinic GmbH, una filiale di Oncare GmbH. In questo contesto, Oncare GmbH fornisce solo la piattaforma tecnica.

Ultimo aggiornamento: giugno 2025.

* * *

Di seguito sono riportate le norme supplementari sulla protezione dei dati per gli utenti negli Stati Uniti d'America:

L'HIPAA protegge le informazioni sanitarie di identificazione personale (PHI) solo se vengono elaborate nel contesto degli Stati Uniti. sistema sanitario da parte di un'entità conforme alla normativa HIPAA, ovvero un'entità coperta o un socio in affari, indipendentemente dalla cittadinanza o dalla residenza dell'interessato.

US Informativa sulla privacy supplementare per gli utenti negli Stati Uniti d'America (HIPAA)

Portata:
Questa sezione integra la Privacy Policy per gli utenti residenti negli Stati Uniti d'America (USA) o per i casi in cui Protected Informazioni sulla salute (PHI) è trattato ai sensi dell'Health Insurance Portability and Accountability Act (HIPAA).

Si applica in tutti gli stati degli Stati Uniti nella misura in cui ONCARE o i partner incaricati trattano i dati sanitari come *socio d'affari* per conto di *Enti coperti* (ad es. medici o cliniche) nell'ambito dei processi terapeutici.

1. Base giuridica negli Stati Uniti

Il trattamento delle informazioni sanitarie personali negli Stati Uniti è disciplinato dal **Legge sulla portabilità e la responsabilità dell'assicurazione sanitaria del 1996 (HIPAA)** e successive modifiche, tra cui, a titolo esemplificativo ma non esaustivo:

- HIPAA **Norma sulla privacy** (45 CFR Parte 160 e Sottoparti A ed E della Parte 164)
- HIPAA **Regola di sicurezza** (Sottoparti A e C della Parte 164)
- **Regola di notifica delle violazioni HIPAA** (Sottoparte D della Parte 164)
- e, inoltre, l'HITECH Act del 2009

Queste norme si applicano indipendentemente dallo stato degli Stati Uniti in cui si trova il paziente o l'agenzia di elaborazione.

2. Il ruolo di ONCARE come socio d'affari

ONCARE GmbH e le società affiliate negli Stati Uniti agiscono esclusivamente come **soci in affari** ai sensi dell'HIPAA quando **fornire servizi in relazione all'elaborazione di informazioni sanitarie protette per conto di fornitori di servizi sanitari (Enti coperti**). Un Contratto di società in affari (BAA) ai sensi del 45 CFR §164.504(e) disciplina gli obblighi di protezione dei dati nei confronti di tali entità. In questo ambito, ONCARE si impegna:

- Fornitura della piattaforma myoncare (video, comunicazione, monitoraggio)
- Elaborazione dati tecnici e hosting
- Fornitura di funzioni di supporto algoritmico (ad es. triage)

ONCARE non fornisce **Servizi medici** e **non prende decisioni mediche** nel senso di diagnosi, terapia o prescrizione.

3. Tipologia di dati trattati (PHI)

Ai fini dell'HIPAA, per PHI si intende qualsiasi informazione che:

- si riferiscono allo stato di salute o al trattamento di un paziente identificabile, e
- in relazione a un *Ente coperto* o il suo socio in affari.

Le PHI elaborate da ONCARE comprendono, in particolare:

- Anamnesi (sintomi, fattori di rischio)
- Dati di monitoraggio (parametri vitali, dati indossabili)
- Interazioni dell'utente all'interno di questionari strutturati o strumenti di triage
- Storie di comunicazione con gli operatori sanitari

4. Diritti dei pazienti ai sensi dell'HIPAA

Tutti gli utenti interessati negli Stati Uniti ha diritto di:

- **Informazione** sulle PHI memorizzate su di lui (45 CFR §164.524)
- **Correzione** di PHI errati o incompleti (45 CFR §164.526)
- **Limitazione** di divulgazione o utilizzo in alcuni casi (45 CFR §164.522)
- **Comunicazione riservata** su richiesta del paziente
- **Opporsi** a determinate divulgazioni (nella misura consentita dalla legge)
- **Contabilità** delle informazioni (45 CFR §164.528)
- **Reclamo** negli Stati Uniti Dipartimento della Salute e dei Servizi Umani (Ufficio per i Diritti Civili)

ONCARE fornisce interfacce tecniche per implementare questi diritti su richiesta.

Per far valere questi diritti, è possibile presentare una richiesta informale tramite l'app myoncare o contattarci via e-mail. L'attuazione avviene solitamente entro 30 giorni in conformità con 45 CFR §164.524 e seguenti. Se la richiesta è complessa, il termine può essere prorogato una volta di altri 30 giorni. A tale scopo, ONCARE fornisce formati di esportazione digitale e interfacce di accesso.

5. Misure di sicurezza in conformità con le regole di sicurezza

ONCARE si impegna a rispettare tutti i requisiti della norma di sicurezza HIPAA, tra cui:

Misure amministrative

- Concetti interni di protezione e accesso ai dati
- Linee guida scritte sulla regolamentazione dell'accesso
- Analisi dei rischi e audit periodici
- Formazione dei dipendenti con focus HIPAA

Inoltre, ONCARE si impegna a condurre regolarmente una "Valutazione dei rischi per la sicurezza" strutturata in conformità con 45 CFR §164.308(a)(1)(ii)(A) per identificare, valutare e intraprendere le azioni appropriate sui rischi per la sicurezza.

Misure tecniche

- Crittografia di tutte le informazioni sanitarie protette a riposo e in transito
- Controllo degli accessi basato sui ruoli
- Cronologia delle registrazioni e degli accessi
- Autenticazione a due fattori per il personale medico

Misure fisiche

- Posizioni sicure dei server con il controllo degli accessi
- Concetti relativi al ripristino di emergenza
- Restrizioni di accesso all'hardware e agli endpoint

6. Protezione dei dati nella valutazione automatizzata

La piattaforma myoncare contiene una funzione di triage strutturata che valuta le informazioni del paziente (ad es. sintomi) in base a criteri definiti e crea **una valutazione tecnica dei rischi**.

Questa caratteristica:

- **non sostituisce una diagnosi medica**,
- **non decide autonomamente in merito al trattamento o all'intervento**,
- **informa solo i fornitori di servizi autorizzati** (entità interessate) di informazioni potenzialmente pertinenti.

ONCARE non si assume alcuna responsabilità medica per le decisioni prese da medici o cliniche sulla base di queste informazioni.

7. Divulgazione di informazioni sanitarie protette e altri usi

ONCARE condivide le PHI solo con:

- agli operatori sanitari idonei nell'ambito delle cure,
- alle autorità di vigilanza se richiesto dalla legge,
- per gli incidenti di sicurezza ai sensi del **Regola di notifica delle violazioni** (entro 60 giorni dalla conoscenza ai sensi del 45 CFR §164.404),
- mai per scopi pubblicitari, di distribuzione o di utilizzo da parte di terzi senza il consenso espresso e documentato del paziente.

Qualsiasi divulgazione o utilizzo di PHI per la ricerca, il marketing o altri scopi di terze parti avverrà solo previa autorizzazione documentata in conformità con 45 CFR §164.508. In mancanza di tale consenso esplicito, tale divulgazione non avrà luogo.

Utilizzo di dati anonimizzati per scopi commerciali
ONCARE può utilizzare i dati sanitari e di utilizzo che sono stati resi anonimi in conformità con la norma sulla privacy HIPAA (45 CFR §164.514) per analisi interne, miglioramento della piattaforma, sviluppo di nuovi servizi sanitari e altri scopi commerciali.

Una volta resi anonimi, i dati non sono più considerati informazioni sanitarie protette (PHI) e non sono soggetti alle protezioni della norma sulla privacy HIPAA.

8. Contatto per l'esercizio dei diritti

Responsabile per le questioni relative all'HIPAA:
ONCARE GmbH
Balanstraße 71a80339 Monaco di BavieraGermaniaE-mail: privacy@myoncare.com

Stati Uniti I cittadini possono anche contattare il **Stati Uniti Dipartimento della Salute e dei Servizi Umani – Ufficio per i Diritti Civili (OCR)** direttamente con i reclami: https://www.hhs.gov/ocr/

9. Integrazione di fornitori terzi, dati del webshop e disclaimer

9.1 Coinvolgimento di fornitori tecnici terzi (produttori di dispositivi, distributori di dispositivi medici e laboratori)

Nell'ambito della piattaforma myoncare e della sua affiliata myon.clinic, **fornitori terzi come produttori di dispositivi, distributori di dispositivi medici o laboratori medici** Se necessario, può essere collegato al sistema. Ciò avviene esclusivamente per supportare un'assistenza responsabile dal punto di vista medico e si basa sulle istruzioni dei rispettivi *Enti coperti*.

I fornitori di servizi di terze parti collegati elaborano le informazioni sanitarie di identificazione personale (PHI) solo in base a un accordo contrattuale e in conformità con i requisiti HIPAA. L'utente è inoltre soggetto ai requisiti di protezione dei dati di 45 CFR §164.502(e) in qualità di *terzista* di un socio in affari e sono vincolati da corrispondenti **contratti di subfornitura (sub-BAA**).

9.2 Raccolta dei dati nell'ambito delle offerte del negozio online

Quando si acquistano programmi di salute digitale, i cosiddetti programmi di salute digitale. **Vie**o prodotti affiliati tramite il negozio online della filiale **myon.clinic**, i dati personali, comprese le PHI, possono essere trattati ai fini dell'elaborazione e del mantenimento di questi programmi. Ciò vale in particolare:

- Dati di utilizzo della funzionalità Pathway,
- sintomi o dati diagnostici specificati,
- eventuali codici sanitari o informazioni sul prodotto riscattati.

La raccolta viene effettuata nel rispetto delle norme sulla privacy e sulla sicurezza HIPAA ed esclusivamente per uno scopo specifico. La divulgazione a fornitori terzi avverrà solo sulla base di un sub-BAA esistente o con il consenso documentato.

Qualsiasi divulgazione di PHI (informazioni sanitarie protette) al di fuori della catena contrattuale (ad es. per ricerca o marketing) richiede un documento **"autorizzazione"** secondo 45 CFR §164.508.

9.3 Esclusione di responsabilità per la valutazione medica e gli effetti collaterali

ONCARE GmbH e le sue società affiliate non si assumono **qualsiasi valutazione medica o obbligo di segnalare reazioni avverse ai farmaci, effetti collaterali del prodotto o altri rischi correlati alla salute.**

Responsabilità legale per:

- la diagnosi e la selezione di un percorso o di un prodotto,
- la valutazione dei rischi o delle controindicazioni,
- nonché i requisiti di legge **segnalazione degli effetti indesiderati** o eventi di sicurezza alle autorità di regolamentazione o ai produttori

spetta esclusivamente al medico curante o all'offerente **Ente coperto** o il produttore del dispositivo o del farmaco responsabile.

La piattaforma **fornisce solo l'infrastruttura tecnica** e non si assume alcuna responsabilità medica o normativa per il contenuto, i risultati o le conseguenze di qualsiasi applicazione da parte di pazienti o fornitori di servizi.

Conformità alle regole di prelazione e alle leggi statali

L'Health Insurance Portability and Accountability Act (HIPAA) fornisce un **Livello minimo di protezione dei dati ai sensi della legge federale** ciò si applica in tutti gli Stati Uniti Stati. Allo stesso tempo, il 45 CFR §160.203 consente il cosiddetto **prelazione**, vale a dire che normative più severe da parte dei singoli stati possono prevalere sull'HIPAA sotto determinati aspetti se:

- garantire una maggiore protezione degli interessati, o
- requisiti speciali per i dati sanitari o i dati sanitari elettronici.
- ONCARE e le sue affiliate si impegnano espressamente a rispettare tutte le leggi federali pertinenti, tra cui, a titolo esemplificativo ma non esaustivo:

- **Legge sulla privacy dei consumatori della California (CCPA/CPRA)**
- **Legge sulla privacy medica del Texas (TMPA)**
- **Legge sullo SHIELD di New York**
- **Normative sulla sicurezza dei dati del Massachusetts**
- nonché leggi comparabili sulla protezione dei dati a livello statale

Nella misura in cui ONCARE agisce per conto delle Entità coperte, il trattamento viene effettuato in conformità con l'HIPAA e gli standard statali applicabili in materia di protezione dei dati, a condizione che questi siano più severi dei requisiti HIPAA. In caso di scostamenti, la normativa che **offre al paziente interessato un livello più elevato di protezione dei dati** vale sempre.

Oltre alle normative HIPAA a livello nazionale, nei singoli stati si applicano ulteriori leggi sulla protezione dei dati, come la California, New York o il Texas. Nella misura in cui queste leggi hanno requisiti più severi rispetto all'HIPAA, hanno la precedenza. In questi casi, ONCARE rispetterà le più severe leggi applicabili.

11. Esercizio dei diritti HIPAA (procedure, verifica dell'identità, limiti di tempo)

Utenti residenti negli Stati Uniti o i cui dati sono trattati da U.S. le entità interessate hanno i diritti di cui alla Sezione 4 della presente Informativa sulla privacy in conformità con l'HIPAA.

Per l'esercizio di tali diritti si applicano le seguenti disposizioni:

11.1 Applicazione

I diritti HIPAA possono essere esercitati da:

- richiesta scritta via e-mail a: **privacy@myoncare.com**
- Richiesta scritta relativa al rispettivo fornitore di cure (*Ente coperto*)

11.2 Verifica dell'identità

A tutela dell'interessato, l'eventuale richiesta di esercizio dei diritti sarà evasa solo dopo **verifica dell'identità riuscita**. Le possibili misure includono:

- Confronto con i dati utilizzati in fase di registrazione
- Presentazione di un documento d'identità valido con foto (in caricamento sicuro)
- Conferma del medico curante

11.3 Termini di trattamento

ONCARE elabora le richieste:

- **entro 30 giorni di calendario** a decorrere dalla data di ricevimento della domanda,
- Estensione per **altri 30 giorni** è consentito una sola volta; il richiedente è informato per iscritto e riceve la giustificazione
- tutte le richieste e le risposte saranno documentate e archiviate in conformità con 45 CFR §164.530(j).

12. Elaborazione dei dati al di fuori degli Stati Uniti (offshoring / localizzazione dei dati)

In alcuni casi, l'elaborazione delle informazioni sanitarie protette può essere effettuata per conto di una società statunitense Ente coperto **al di fuori degli Stati Uniti**soprattutto:

- da ONCARE GmbH, con sede in Germania (UE),
- fornire servizi di infrastruttura tecnica, hosting, supporto e sviluppo di prodotti.

Questo trattamento transfrontaliero viene effettuato esclusivamente:

- sulla base di un **Contratto di società in affari** (BAA),
- con documentazione esplicita nel piano di gestione dei rischi HIPAA dell'entità coperta,
- conformità alla norma di sicurezza HIPAA e alle norme **misure di sicurezza secondo lo standard europeo GDPR**soprattutto:
  - → Crittografia end-to-end (AES-256),
  - → Limitazione dell'accesso secondo il principio del need-to-know,
  - → Registrazione di tutti gli accessi con audit trail,
  - → Archiviazione dei dati solo su server con controllo degli accessi fisici e certificazione ISO 27001.

PHI è **non memorizzato su sistemi al di fuori degli Stati Uniti senza adeguate misure tecniche di protezione** e la tutela contrattuale.

Garanzie amministrative

ONCARE ha implementato misure amministrative ai sensi del 45 CFR §164.308 per tutti i servizi relativi agli Stati Uniti, tra cui:

- **Responsabili della protezione dei dati e funzionari HIPAA a livello aziendale**
- **Politiche sulla privacy e sulla sicurezza**, con versione, documentato e supportato da formazione
- **Formazione obbligatoria per tutti i dipendenti** che lavorano con i dati sanitari degli Stati Uniti (almeno una volta all'anno)
- **Norme sulle sanzioni** per violazioni della protezione dei dati come definito da 45 CFR §164.530(e)
- **Valutazione del sistema basata sul rischio e valutazioni delle vulnerabilità**, almeno una volta all'anno o in caso di modifiche significative del sistema

Tutti i processi sono documentati in un **Manuale di conformità HIPAA**, che viene regolarmente aggiornato e riesaminato nell'ambito dell'audit interno.

14. Misure di sicurezza tecniche per le norme di sicurezza HIPAA

ONCARE ha pienamente implementato le misure tecniche di protezione in conformità con 45 CFR §164.312:

Categoria	Misura
Controllo di accesso	Accesso basato sui ruoli, ID utente univoci, disconnessione automatica dalle sessioni, procedure di accesso di emergenza
Controlli di controllo	Registrazione completa del sistema e degli accessi con valutazione periodica
Controlli di integrità	Controlli di integrità basati su hash e controllo della versione per dati medici critici
Autenticazione	Autenticazione a due fattori per il personale medico e gli amministratori
Sicurezza della trasmissione	Crittografia TLS 1.3 durante la trasmissione, protezione VPN per tutti i fornitori di servizi esterni

Queste misure si applicano a tutti i sistemi che memorizzano, elaborano o trasmettono PHI. L'attuazione è assicurata annualmente da test tecnici di penetrazione e da un **Analisi dei rischi conforme a HIPAA** .

***