DATENSCHUTZERKLÄRUNG FÜR EUROPA

Willkommen bei myoncare, dem digitalen Gesundheitsportal für eine effiziente und bedarfsgerechte Patientenversorgung.
Für uns bei der Oncare GmbH (im Folgenden "**ONCARE**" oder "**wir**", "**Wir**", "**unser**"), ist der Schutz Ihrer Privatsphäre und aller personenbezogenen Daten, die sich während der Nutzung des myoncare Portals auf Sie beziehen, von großer Bedeutung und Wichtigkeit. Wir sind uns der Verantwortung bewusst, die sich aus der Bereitstellung und Speicherung Ihrer personenbezogenen Daten im myoncare Portal ergibt. Daher sind unsere Technologiesysteme, die für die myoncare-Dienste verwendet werden, nach höchsten Standards eingerichtet und die rechtmäßige Verarbeitung der Daten steht im Mittelpunkt unseres ethischen Verständnisses als Unternehmen.

Wir verarbeiten Ihre personenbezogenen Daten in Übereinstimmung mit den geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, insbesondere der EU-Datenschutz-Grundverordnung ("**DSGVO")** und die für uns geltenden länderspezifischen Gesetze. In dieser Datenschutzerklärung erfahren Sie, warum und wie **ONCARE** Ihre personenbezogenen Daten verarbeitet, die wir von Ihnen erfassen oder die Sie uns zur Verfügung stellen, wenn Sie sich für die Nutzung des myoncare Portals entscheiden. Insbesondere finden Sie eine Beschreibung der Art der personenbezogenen Daten, die wir erheben und verarbeiten, sowie den Zweck und die Grundlage, auf der wir die personenbezogenen Daten verarbeiten; darüber hinaus finden Sie hier die Rechte, die Ihnen zustehen.

Bitte lesen Sie die Datenschutzrichtlinie sorgfältig durch, um sicherzustellen, dass Sie jede Bestimmung verstehen. Nachdem Sie die Datenschutzrichtlinie gelesen haben, haben Sie die Möglichkeit, der Datenschutzrichtlinie zuzustimmen und in die Verarbeitung Ihrer personenbezogenen Daten, wie in der Datenschutzrichtlinie beschrieben, einzuwilligen. Wenn Sie Ihre Einwilligung erteilen, wird die Datenschutzerklärung Bestandteil des Vertrags zwischen Ihnen und ONCARE.

Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.

DEFINITIONEN

„App-Nutzer" ist jeder Benutzer der myoncare App (Ihr Patient).

„Blockchain-Technologie" Das myoncare-System enthält eine zusätzliche Datenbank, in der die Daten aller Installationen gespeichert werden.

"Careplan-Anbieter" bezeichnet Sie oder einen anderen Dienstleister oder Dritten (z. B. Hersteller von Medizinprodukten, Pharmaunternehmen), der Pflegepläne über den myoncare Store oder andere Mittel des Datenaustauschs anderen Nutzern des Portals zur Verfügung stellt.

"Careplan-Nutzer" bezeichnet Sie oder einen anderen Dienstleister (Portalnutzer), der einen Pflegeplan ("Pathway") für die Behandlung seiner registrierten Patienten verwendet.

"Pathway" ist ein standardisierter Behandlungsplan, der bestehend aus mehreren, ggfs. zeitlich aneinander gereihten Caretasks, die Schritte für Diagnosen und Therapien festlegen kann. **„Caretasks"** sind spezifische Aufgaben oder Handlungen innerhalb eines Pathways, die von den beteiligten Leistungserbringern, dem Pflegepersonal oder dem Patienten selbst durchgeführt werden müssen.

„**Leistungserbringer**" bezeichnet Sie oder einen anderen Arzt, eine Klinik, eine Gesundheitseinrichtung oder einen anderen Angehörigen der Gesundheitsberufe, der allein oder im Auftrag von Ihnen oder einem anderen Arzt, einer Klinik oder einer Gesundheitseinrichtung (beabsichtigter Benutzer) handelt.

„**myoncare-App**" bezeichnet die mobile myoncare-Anwendung für Patienten, die die von ONCARE angebotenen Dienste über die App nutzen möchten.

„**myoncare Store**" ist die von **ONCARE** betriebene Plattform, die digitale Versorgungskonzepte (Behandlungspläne) für die Behandlung Ihrer registrierten Patienten über das myoncare-Portal bereitstellt.

„**myoncare-Tools**" meint die myoncare-App und das myoncare-Portal zusammen.

"**myoncare PWA**" bezeichnet die myoncare Progressive Web App Anwendung für Patienten, die die von ONCARE angebotenen Dienste über die PWA und nicht über die myoncare App nutzen möchten.

"**myoncare Portal**" ist das myoncare-Webportal, das für die professionelle Nutzung durch Portalnutzer bestimmt ist und als Schnittstelle zwischen Portal-Nutzern und App-Nutzer dient.

"**myoncare Services**" bezeichnet die Dienste, Funktionalitäten und sonstigen Angebote, die den Portalnutzern über das myoncare Portal und/oder den App-Nutzern über die myoncare App angeboten werden oder angeboten werden können.
"**ONCARE**" bezeichnet die ONCARE GmbH, Deutschland.

"**Portal-Benutzer**" bezeichnet Sie oder einen anderen Dienstleister, der das webbasierte myoncare Portal nutzt.

"**Datenschutzerklärung für Patienten**" bezeichnet die Datenschutzrichtlinie, die die Erfassung, Verwendung und Speicherung der persönlichen (Gesundheits-) Informationen von Patienten beschreibt, die die myoncare App verwenden. Unser Angebot richtet sich laut Nutzungsbedingungen nur an Personen ab 18 Jahren. Dementsprechend werden keine personenbezogenen Daten von Kindern und Jugendlichen unter 18 Jahren gespeichert und verarbeitet.

"**Datenschutzerklärung**" bezeichnet diese Erklärung, die Ihnen als Nutzer des myoncare-Portals zur Verfügung gestellt wird und die beschreibt, wie wir Ihre personenbezogenen Daten sammeln, verwenden und speichern, und Sie über Ihre umfassenden Rechte informiert.

"**Nutzungsbedingungen**" bezeichnet die Nutzungsbedingungen für die Nutzung des myoncare Portals.

VERARBEITUNG VON (BEHANDLUNGS-)DATEN

Die Oncare GmbH, eine beim Amtsgericht München unter der Registernummer 219909 eingetragene Gesellschaft mit Sitz in der Balanstraße 71a, 81541 München, Deutschland, bietet und betreibt das interaktive Webportal myoncare Portal (für medizinisches Fachpersonal) und die mobile Anwendung myoncare App (für Patienten) als Zugang zu den myoncare-Dienstleistungen. Diese **Datenschutzerklärung** gilt für alle personenbezogenen Daten, die von ONCARE im Zusammenhang mit der Nutzung des **myoncare Portals** verarbeitet werden. Für die Nutzung der **myoncare App** durch Patienten finden Sie eine separate Datenschutzerklärung für Patienten **hier**.

WAS SIND PERSONENBEZOGENE DATEN

"**Personenbezogene Daten**" bezeichnet alle Informationen, die es ermöglichen, eine natürliche Person zu identifizieren. Dazu gehören unter anderem Ihr Name, Ihr Geburtstag, Ihre Adresse, Ihre Telefonnummer, Ihre E-Mail-Adresse und Ihre IP-Adresse.

"**Gesundheitsdaten**" sind personenbezogene Daten, die sich auf die physische und psychische Gesundheit einer natürlichen Person beziehen, einschließlich der Bereitstellung von Gesundheitsdiensten, die Informationen über ihren Gesundheitszustand offenbaren.

Daten sind als "**anonym**" anzusehen, wenn kein persönlicher Bezug zu der Person/dem Nutzer hergestellt werden kann.
Im Gegensatz dazu sind „**pseudonymisierte**“ Daten Daten, aus denen ein persönlicher Bezug oder persönlich identifizierbare Informationen durch einen oder mehrere künstliche Identifikatoren oder Pseudonyme ersetzt werden, die aber im Allgemeinen durch den Identifikatorschlüssel re-identifiziert werden können. (im Sinne von Art. 4 Nr. 5 DSGVO).

Myoncare PWA

Eine Progressive Web App (PWA) ist eine Website, die aussieht und die Funktionalität einer mobilen App hat. PWAs wurden entwickelt, um die nativen Funktionen mobiler Geräte zu nutzen, ohne dass ein App Store erforderlich ist. Das Ziel von PWAs ist es, den Unterschied zwischen Apps und dem traditionellen Web zu kombinieren, indem die Vorteile nativer mobiler Apps in den Browser gebracht werden. Die PWA basiert auf der Technologie von "React ". "React" ist eine Open-Source-Software für PWA-Anwendungen.

Um die Funktion **myoncare PWA** nutzen zu können benötigen Patienten einen Computer oder ein Smartphone und eine aktive Internetverbindung. Es ist nicht erforderlich, eine App herunterzuladen.

Einige der myoncare App-Dienste können nicht innerhalb der **myoncare PWA** genutzt werden, Details dazu siehe die Beschreibung unten. Dabei handelt es sich um die folgenden Dienstleistungen oder Spezifikationen:
-Chatten mit **Leistungserbringern**;
-Video;
-Sicherheits-PIN-Codes;
-Tracking von Aktivitätsdaten (z. B. über AppleHealth, GoogleFit, Withings).
Die folgenden Informationen über die **myoncare App** gilt auch für die **myoncare PWA**, sofern in diesem Abschnitt nichts anderes beschrieben ist.

WELCHE PERSONENBEZOGENEN DATEN WERDEN BEI DER NUTZUNG DER MYONCARE APP VERWENDET?

Wir können die folgenden Datenkategorien über Sie bei der Nutzung der **myoncare App** verarbeiten:

Operative Daten: Personenbezogene Daten, die Sie uns bei der Registrierung in unserem **myoncare portal**, bei der Kontaktaufnahme zu Problemen mit dem Portal oder bei sonstigen Interaktionen mit uns zum Zweck der Nutzung des Portals zur Verfügung stellen.

Behandlungsdaten: Sie erheben personenbezogene Daten Ihrer Patienten, wie Name, Alter, Größe, Gewicht, Indikation, Krankheitssymptome und andere Informationen im Zusammenhang mit der Behandlung Ihrer Patienten (z.B. in einem Careplan) in dem **myoncare Portal**. Aktivitätsdaten Ihrer verbundenen Patienten werden Ihnen in Ihrem **myoncare Portal** verfügbar gemacht.

Kommerzielle Store-Daten: Personenbezogene Daten, die von uns bei der Nutzung des **myoncare Stores** verarbeitet werden, entweder im Zusammenhang mit der Autorenschaft von Behandlungsplänen oder dem Kauf von Behandlungsplänen. Die Verwendung des **myoncare Store** erfordert die Verarbeitung Ihres Namens und anderer Kontaktinformationen sowie Zahlungsdaten (Zahlungsinformationen nur, wenn der Pflegeplan kostenpflichtig ist).

Aktivitätsdaten: Personenbezogene Daten, die von uns verarbeitet werden, wenn ein **App-Nutzer** die **myoncare-App** mit einer Gesundheitsanwendung (z. B. AppleHealth, GoogleFit, Withings) verbindet. Die Aktivitätsdaten Ihrer angeschlossenen Patienten werden Ihnen in Ihrem **myoncare Portal** verfügbar gemacht.

Kommerzielle und nicht-kommerzielle Forschungsdaten:
Wir verarbeiten Ihre personenbezogenen Daten in anonymisierter/pseudonymisierter Form, um zusammenfassende wissenschaftliche Berichte zu analysieren und zu erstellen, um Produkte, Behandlungen und wissenschaftliche Ergebnisse zu verbessern.

Produktsicherheitsdaten Personenbezogene Daten, die zur Erfüllung unserer gesetzlichen Verpflichtungen als Hersteller der **myoncare App** als Medizinprodukt verarbeitet werden. Darüber hinaus können Ihre personenbezogenen Daten verarbeitet werden, falls Sie einen Vorfall melden, um die Rechtssicherheit oder die Wachsamkeit von Medizinprodukte- oder Pharmaunternehmen zu gewährleisten.

Kostenerstattungsdaten: Personenbezogene Daten, die für den Erstattungsprozess erforderlich sind.

BLOCKCHAIN-TECHNOLOGIE

Blockchain-**Technologie** („**Blockchain**“) (Europäisches Patent Nr. 4 002 787) ist ein optionaler Dienst, der nicht verpflichtend ist. Es liegt an Ihnen, dem **Leistungserbringer**, sich für die Nutzung der Blockchain-Lösung zu entscheiden. Die **Blockchain** basiert auf der Technologie von Hyperledger Fabric. Hyperledger Fabric ist eine Open-Source-Software für Blockchain-Implementierungen auf Unternehmensebene. Sie bietet eine skalierbare und sichere Plattform, die Blockchain-Projekte unterstützt.

Die **Blockchain** im myoncare-System ist eine zusätzliche Datenbank, in der Daten aus der Anwendung gespeichert werden. Alle Daten der Blockchain **werden** in der Bundesrepublik Deutschland gespeichert. Es handelt sich um ein private **Blockchain** ("**Private Blockchain**"), es erlaubt nur die Eingabe ausgewählter verifizierter Teilnehmer und es ist möglich, Einträge nach Bedarf zu überschreiben, zu bearbeiten oder zu löschen.

Die **Blockchain** besteht im Allgemeinen aus digitalen Daten in einer Kette von Paketen, die „Blöcke“ genannt werden und die entsprechenden Transaktionen speichern. Die Art und Weise, wie diese Blöcke miteinander verbunden sind, ist chronologisch. Der erste Block, der erstellt wird, wird als Genesis-Block bezeichnet, und jeder danach hinzugefügte Block hat einen kryptografischen Hash, der sich auf den vorherigen Block bezieht, sodass Transaktionen und Informationsänderungen auf den Genesis-Block zurückgeführt werden können. Alle Transaktionen innerhalb der Blöcke werden durch einen Blockchain-Konsensmechanismus validiert und verifiziert, um sicherzustellen, dass jede Transaktion unverändert bleibt.

Jeder Block enthält die Liste der Transaktionen, einen Zeitstempel, einen eigenen Hash und den Hash des vorherigen Blocks. Ein Hash ist eine Funktion, die digitale Daten in eine alphanumerische Kette umwandelt. In diesem Fall kann der Block nicht mehr mit den anderen synchronisiert werden. Wenn eine unbefugte Person versucht, die Daten eines einzelnen Blocks zu ändern, ändert sich auch der Hash des Blocks und die Verknüpfung zu diesem Block geht verloren. Wenn alle Knoten (Netzwerkknoten) versuchen, ihre Kopien zu synchronisieren, wird festgestellt, dass die geänderte Kopie geändert wurde, und das Netzwerk betrachtet diesen Knoten als fehlerhaft. Dieser technische Prozess verhindert, dass Unbefugte die Inhalte der Blockchain-Kette manipulieren können.

Unsere **Blockchain** ist eine **private Blockchain**. Eine private **Blockchain** ist dezentralisiert. Dabei handelt es sich um ein sogenanntes Distributed-Ledger-System (digitales System zur Erfassung von Transaktionen), das als geschlossene Datenbank fungiert. Im Gegensatz zu öffentlichen **Blockchains**, die „unauthorisiert“ sind, sind **private Blockchains** „autorisiert“, da eine Autorisierung erforderlich ist, um Nutzer zu werden. Im Gegensatz zu öffentlichen **Blockchains**, die für jeden öffentlich zugänglich sind, ist der Zugang zu **privaten Blockchains** von einer Autorisierung abhängig, um Nutzer zu werden. Diese Struktur ermöglicht es, die Sicherheit und Unveränderlichkeit der **Blockchain-Technologie** zu nutzen und gleichzeitig datenschutzkonform zu bleiben, insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) einzuhalten. Private Blockchain-Datensätze können bearbeitet, geändert oder gelöscht werden. Eine Löschung bedeutet in diesem Zusammenhang, dass der Referenzwert auf die UUID (Universally Unique Identifier) in der Datenbank des **Leistungserbringer** gelöscht wird. Darüber hinaus wird der Hash in der Blockchain-Datenbank anonymisiert, so dass dieser Gesamtprozess konform mit der Datenschutz-Grundverordnung ist und die Rechte einer betroffenen Person gewährleistet sind (Recht auf Löschung "Recht auf Vergessenwerden", Art. 17 DSGVO).

Art der Daten, die in der Blockchain gespeichert und verarbeitet werden:

-Patienten-UUID
-Institutionen/**Leistungserbinger** UUID
-Asset-UUID
-Hash von **caretask** und Asset-Daten.
(*UUID: Universeller eindeutiger Identifikator*).

Die in der **Blockchain** gespeicherten Daten sind pseudonymisiert.
Unsere **Blockchain** ist darauf ausgelegt, den Datenschutz in Bezug auf Datenintegrität, Patientenprofile, Vermögenswerte sowie zugewiesene **Care Tasks** und Medikamente zu gewährleisten. Um mit der **Blockchain** zu kommunizieren, muss der Benutzer eine Reihe von öffentlichen und privaten Schlüsseln registrieren. Um mit der **Blockchain** zu kommunizieren, benötigt der Benutzer mehrere öffentliche und private Schlüssel; der Registrierungsprozess generiert Zertifikate, die in einer separaten Datenbank des **Leistungserbringers** und auf dem Mobiltelefon des Patienten gespeichert werden. Eine Sicherungskopie des Patientenschlüssels wird verschlüsselt in der Datenbank des **Leistungserbringers** gespeichert, auf die nur der Patient zugreifen kann.

Bei der Überprüfung der Zustimmung zum Datenschutz, falls der **Leistungserbringer** mit dem Patienten kommunizieren möchte, überprüft das System, ob der Patient der Datenschutzrichtlinie des **Leistungserbringers** zugestimmt hat. Die **Blockchain** dient somit dazu, die Integrität und Verantwortlichkeit des Protokolls sicherzustellen, um zu gewährleisten, dass der Patient die Datenschutzrichtlinie akzeptiert hat.

Wenn ein **Leistungserbringer** eine neue Version einer Datenschutzrichtlinie hochlädt, wird der Hash der Datei auf der **Blockchain** gespeichert, und nachdem der

Patient der Datenschutzrichtlinie zugestimmt hat, wird diese Interaktion auf der **Blockchain** gespeichert. Jedes Mal, wenn eine Kommunikation mit dem Patienten erfolgt, antwortet die **Blockchain**, indem sie den Hash mit einer Markierung vergleicht, die anzeigt, ob die Zustimmung des Patienten für die aktuelle Datenschutzrichtlinie noch gültig ist.
Die Integrität des Patientenprofils wird auch durch die Blockchain bei der Patientensynchronisation sichergestellt. Der **Leistungserbringer** erkennt sofort, wenn das Patientenprofil nicht synchronisiert oder nicht mit dem Profil auf dem Mobiltelefon übereinstimmt, indem er den Hash des Patientenprofils in der Blockchain vergleicht. Auf diese Weise erreicht der **Leistungs**erbringer eine hinreichende Aktualität in Bezug auf das Patientenprofil.

myoncare Portal:
Wenn sich der **Leistungserbringer** für die Blockchain-Lösung entscheidet, implementiert ONCARE ein zusätzliches Tool, genannt "Adapter Service", dass für die Kommunikation mit der **Blockchain** verwendet wird. Die Blockchain-Instanz wird von ONCARE gehostet.

myoncare App:
Patienten können sich mit dem Phone Manager-Tool, das ebenfalls von ONCARE gehostet wird, mit derselben Blockchain-Instanz verbinden. Dieser Service wird ebenfalls von ONCARE gehostet.

Rechtfertigung der Verarbeitung: Die Verarbeitung von Daten durch ONCARE im Auftrag des **Leistungserbringers** erfolgt auf der Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

VERARBEITUNG VON OPERATIVEN DATEN

Falls Sie eine Kontaktperson für den Betrieb des Portals an Ihrem Standort/Ihrer Praxis sind (z. B. IT-Administrator, ernannte medizinische Fachkraft), können Sie uns bestimmte personenbezogene Daten zur Verfügung stellen, wenn Sie uns kontaktieren, um die Funktionen und die Nutzung des Portals zu verstehen oder zu besprechen, oder im Falle einer Serviceanfrage.

Im Falle einer Serviceanfrage können auch folgende personenbezogene Daten von autorisierten ONCARE-Mitarbeitern eingesehen werden:

Ihre personenbezogenen Daten, die Sie uns für die Registrierung und/oder Anmeldung in unserem Portal zur Verfügung gestellt haben (z.B. Name, Geburtsdatum, Profilbild, Kontaktdaten).

Autorisierte ONCARE-Mitarbeiter, die zum Zwecke der Bearbeitung einer Serviceanfrage auf Ihre Datenbank zugreifen dürfen, sind vertraglich verpflichtet, alle personenbezogenen Daten streng vertraulich zu behandeln.

Wichtige Erläuterungen zu Push-Benachrichtigungen und E-Mails
Im Rahmen Ihrer Unterstützung durch myoncare möchten wir Sie darüber informieren, wie wir mit Benachrichtigungen umgehen und wichtige Informationen, die wir Ihnen zukommen lassen.

1. **Push-Benachrichtigungen**:
   - Wir senden Ihnen Push-Benachrichtigungen über unsere **myoncare-PWA** (Progressive Web App) und die **myoncare-App**, um Sie über Aufgaben, Termine und wichtige Updates zu informieren.
   - Sie haben die Möglichkeit, diese Push-Benachrichtigungen in den Einstellungen Ihrer App zu deaktivieren.
2. **E-Mail-Benachrichtigungen**:
   - Unabhängig davon, ob Sie Push-Benachrichtigungen aktiviert oder deaktiviert haben, senden wir Ihnen weiterhin wichtige Informationen und Erinnerungen per E-Mail.
   - So stellen Sie sicher, dass Sie keine wichtigen Benachrichtigungen verpassen und Ihr Support reibungslos läuft.

Warum wir das tun:

- Unser Ziel ist es, dass Sie stets über Ihre Aufgaben und wichtige Updates informiert sind, um Ihre Pflege optimal zu unterstützen.

E-Mails sind ein zuverlässiger Weg, um sicherzustellen, dass wichtige Informationen Sie erreichen, auch wenn Push-Benachrichtigungen deaktiviert sind.

Ihre Handlungsoptionen:

- Wenn Sie keine Push-Benachrichtigungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare-App** deaktivieren.

- Bitte stellen Sie sicher, dass Ihre E-Mail-Adresse korrekt und aktuell ist, um einen reibungslosen Empfang unserer Nachrichten zu gewährleisten.
- Wenn Sie keine E-Mail-Erinnerungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare-App** deaktivieren.

Bei der Verarbeitung von Betriebsdaten fungiert ONCARE als Datenverantwortlicher, der für die rechtmäßige Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist.

Arten von Daten: E-Mail-Adresse, Geburtsdatum, Datum der Registrierung, Ihre IP-Adresse, vom Portal generierte Pseudoschlüssel.

Die App verwendet die Google Maps API, um geografische Informationen zu verwenden. Bei der Nutzung von Google Maps werden von Google auch Daten über die Nutzung der Kartenfunktionen erhoben, verarbeitet und genutzt. Nähere Informationen über den Umfang, die Rechtsgrundlage und den Zweck der Datenverarbeitung durch Google sowie die Speicherdauer finden Sie in der Datenschutzerklärung von Google.

Zwecke der Verarbeitung von operativen Daten: Wir verwenden die Betriebsdaten, um die Funktionalitäten der **myoncare Portal** aufrechtzuerhalten und um bei Bedarf oder von Ihnen initiiert direkt mit Ihnen in Kontakt zu treten (z. B. bei Änderung der Allgemeinen Geschäftsbedingungen, notwendigem Support, technischen Problemen usw.). Darüber hinaus werden personenbezogene Daten (E-Mail-Adresse) im Rahmen der Zwei-Faktor-Authentifizierung jedes Mal verarbeitet, wenn Sie sich in das **myoncare-Portal** einloggen.

Rechtfertigung der Verarbeitung: Die Verarbeitung von Betriebsdaten ist auf der Grundlage von Art. 6 Abs. 1 lit. b DSGVO für die Erfüllung des Vertrages, den Sie mit ONCARE zum Zwecke der Nutzung der **myoncare Portal** abschließen, gerechtfertigt.

IP GEOLOKALISIERUNG

Wir verwenden für unsere Dienste eine Geolokalisierungsanwendung. Wir verwenden ipapi (bereitgestellt von apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Wien, Österreich) und Geoapify (zur Verfügung gestellt von Keptago Ltd., N. Nikolaidi und T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Zypern), um den Standort von Patientenbenutzern zu identifizieren. Wir verwenden sie, um unsere Anwendungen zu sichern und den Standort des Patientenbenutzers zu überprüfen, um sicherzustellen, dass die Nutzung unserer Dienste konform ist. Wir kombinieren die von uns gesammelten Informationen nicht mit anderen Informationen über den Benutzer, die ihn identifizieren könnten. Zu den von apilayer verarbeiteten Daten gehören die IP-Adresse des Patienten und weitere Angaben zum Standort. Rechtsgrundlage für die Nutzung ist Art. 6 Abs. 1 lit. f DSGVO. Die Daten werden gelöscht, wenn der mit ihr verbundene Zweck, für den sie erhoben wurden, nicht mehr besteht und keine gesetzliche Aufbewahrungspflicht mehr besteht. Weitere Informationen zu deren Datenschutzrichtlinien finden Sie unter https://ipapi.com/privacy/ und Datenschutzerklärung | Geoapify Standortplattform.

VERARBEITUNG VON (BEHANDLUNGS-)DATEN

Während der Nutzung des **myoncare-Portals** geben Sie persönliche (gesundheitsbezogene) Daten Ihrer Patienten in das **myoncare-Portal** ein (z. B. Bereitstellung eines individuellen Behandlungsplans, Erinnerung zur Medikamenteneinnahme usw.). Darüber hinaus können Sie und Ihre Patienten Dokumente und Dateien in das **myoncare Portal** hochladen und miteinander teilen. Darüber hinaus können Standortfunktionen generiert und implementiert werden:

- Hinzufügen eines Standorts;
- Hochladen des Logos der Website;
- Hinzufügen der Details des Standorts;
- eine Datenschutzerklärung hochladen;

Es ist möglich, weitere Einwilligungsanforderungen für den Patienten zu erstellen, für die der Patient eine Einwilligung erteilen muss, um sich mit der Website zu verbinden.

Eine hochgeladene Datenschutzerklärung wird jedem Patienten angezeigt, der sich mit der Website verbindet. Alle Einwilligungserklärungen müssen in der hochgeladenen Datenschutzerklärung dokumentiert werden. Sobald eine Datenschutzerklärung hochgeladen wurde, kann sie nur durch eine neue Version ersetzt, aber nicht gelöscht werden.
Die Dateien werden in einer Cloud-Datenbank in Deutschland gespeichert. Sie können die gemeinsame Nutzung solcher Dateien mit anderen **Portal-Benutzer** innerhalb Ihrer Einrichtung zu medizinischen Zwecken erlauben. Andere **Portal-Benutzer** haben keinen Zugriff auf diese Dateien.
Ferner können Sie einen Leistungserbringer außerhalb Ihrer Einrichtung (Konsiliararzt) im Rahmen der Behandlung Ihrer Patienten hinzuziehen, sofern Sie der Ansicht sind, eine weitere Fachmeinung dient der Behandlung.

Gemäß der DSGVO sind Sie als Datenbeauftragter für die Verarbeitung von Gesundheitsdaten von Patienten im Rahmen der Nutzung der myoncare-Dienste verantwortlich.

Wir verarbeiten diese personenbezogenen Daten, einschließlich der Gesundheitsdaten des Patienten, im Rahmen einer Vereinbarung mit Ihnen und in Übereinstimmung mit Ihren Anweisungen. Bitte verarbeiten Sie die Daten Ihrer Patienten nur, wenn Sie die erforderliche Dateneinwilligung von diesen Patienten eingeholt haben. ONCARE fungiert als Auftragsverarbeiter in Übereinstimmung mit der separaten Datenverarbeitungsvereinbarung,
die wir mit Ihnen auf Grundlage von Art. 28 DSGVO abgeschlossen haben.

VERARBEITUNG VON KOMMERZIELLEN SPEICHERDATEN

Gilt nur, wenn Sie den myoncare Store als Careplan-Benutzer nutzen.
Der **myoncare Store** ist in das **myoncare-Portal** integriert und bietet den Kauf von Behandlungsplänen (Careplan) an. Nach der Registrierung im **myoncare-Portal** können Sie sich mit Ihren Anmeldedaten mit dem **myoncare Store** verbinden. Sie können den **myoncare Store** nutzen, um Behandlungspläne als Nutzer zu erwerben.

Daten des careplan-Nutzers:

Die Daten des **Careplan-Nutzers**, die der **myoncare Store** während der Nutzung verarbeitet, werden zum Abschluss eines Lizenzvertrags mit dem **Careplan-Anbieter** – in diesem Fall ONCARE – und, falls eine Gebühr fällig ist, zur Abwicklung und Kontrolle des Zahlungsvorgangs zwischen dem **Careplan-Anbieter** – in diesem Fall ONCARE – und dem **Careplan-Nutzer** verarbeitet.

Arten von Daten: Name, Kontaktdaten, Bankverbindung.

Verarbeitung von kommerziellen Store-Daten: Personenbezogene Daten, die von uns bei der Nutzung des **myoncare Stores** im Rahmen des Kaufs von Behandlungsplänen verarbeitet werden. Darüber hinaus werden die Zahlungsdaten (falls eine Nutzungsgebühr erhoben wird) an den **Careplan-Anbieter** weitergeleitet.

Rechtfertigung der Verarbeitung kommerzieller Store-Daten: Die Rechtsgrundlage für die Verarbeitung kommerzieller Store-Daten ist Art. 6 Abs. 1 lit. b DSGVO – die Verarbeitung der Daten dient der Erfüllung des Vertrages zwischen **Careplan-Nutzer** und **careplan-Anbieter** – in diesem Fall ONCARE.

VERARBEITUNG VON AKTIVITÄTSDATEN

Nur zutreffend, wenn Ihre verbundenen App-Nutzer dem Datentransfer zustimmen und diesen aktivieren.

Die **myoncare-Tools** bieten **App-Nutzern** die Möglichkeit, die **myoncare-App** mit bestimmten Gesundheits-Apps (z. B. AppleHealth, GoogleFit, Withings) („**Gesundheits-App**“) zu verbinden, sofern diese vom **App-Nutzer** verwendet werden und die Verbindung vom **App-Nutzer** hergestellt wird. Wenn die Verbindung hergestellt ist, werden die von der **Gesundheits-App** gesammelten Aktivitätsdaten Ihnen zur Verfügung gestellt, um zusätzliche kontextuelle Informationen bezüglich der Aktivität des **App-Nutzers** bereitzustellen. Bitte beachten Sie, dass die Aktivitätsdaten nicht von **myoncare Tools** und sollte daher nicht zu diagnostischen Zwecken als Grundlage für medizinische Entscheidungen verwendet werden.

Die Verarbeitung der Aktivitätsdaten liegt in der Verantwortung Ihrer Patienten.

Arten von Daten: Die Art sowie der Umfang von transferierten Daten hängen von der Entscheidung der **App-Nutzer** ab. Zu den Daten gehören unter anderem Gewicht, Größe, zurückgelegte Schritte, verbrannte Kalorien, Schlafstunden, Herzfrequenz und Blutdruck.

Zweck der Verarbeitung von Aktivitätsdaten: Die Aktivitätsdaten des **App-Nutzers** werden Ihnen zur Verfügung gestellt, um zusätzliche kontextuelle Informationen bezüglich der Aktivität des **App-Nutzers** bereitzustellen. Bitte beachten Sie, dass Aktivitätsdaten nicht von den **myoncare-Tools** validiert werden und nicht für diagnostische Zwecke oder als Grundlage für medizinische Entscheidungen verwendet werden sollten.

Begründung der Verarbeitung:
Der Datenverantwortliche ist der Patient selbst, indem er Ihnen Zugang zu seinen Aktivitätsdaten gewährt, um die geteilten Informationen zu überprüfen. Eine weitere Begründung bedarf es daher nicht.

VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

Gilt nur, wenn Sie die Medizinproduktvariante der myoncare Tools verwenden.

Das **myoncare Portal** und die **myoncare App** werden als Medizinprodukt gemäß den europäischen Medizinproduktevorschriften klassifiziert und vermarktet. Als Hersteller der **myoncare-Tools** müssen wir bestimmten gesetzlichen Verpflichtungen nachkommen (z. B. Überwachung der Funktionalität des Tools, Auswertung von Vorfallberichten, die im Zusammenhang mit der Nutzung des Tools stehen könnten, Nachverfolgung von Nutzern usw.). Zusätzlich ermöglichen die **myoncare-Tools** Ihnen, personenbezogene Daten über bestimmte medizinische Geräte oder Medikamente zu erfassen, die bei der Behandlung Ihrer Patienten verwendet werden. Die Hersteller solcher Medizinprodukte oder Arzneimittel haben auch gesetzliche Verpflichtungen hinsichtlich der Marktüberwachung (z.B. Sammlung und Auswertung von Nebenwirkungsmeldungen).

ONCARE ist der Datenverantwortliche für die Verarbeitung von Produktsicherheitsdaten.

Arten von Daten: Fallberichte, personenbezogene Daten, die in einem Vorfallbericht angegeben wurden, und Ergebnisse der Bewertung, Angaben zum Meldenden.

Verarbeitung von Produktsicherheitsdaten: Wir speichern und bewerten alle personenbezogenen Daten im Zusammenhang mit unseren gesetzlichen Verpflichtungen als Hersteller eines Medizinprodukts und übermitteln diese personenbezogenen Daten (soweit möglich nach Pseudonymisierung) an zuständige Behörden, Benannte Stellen oder andere Datenverantwortliche mit Aufsichtspflichten. Darüber hinaus speichern und übertragen wir personenbezogene Daten im Zusammenhang mit medizinischen Geräten und/oder Medikamenten, wenn wir Mitteilungen von Ihnen als Meldender solcher Informationen, von Ihrem Patienten oder von Dritten (z. B. unseren Vertriebspartnern oder Importeuren der **myoncare-Tools** in Ihrem Land) erhalten, die dem Hersteller des Produkts gemeldet werden müssen, damit dieser seinen gesetzlichen Verpflichtungen zur Produktsicherheit nachkommen kann.

Begründung für die Verarbeitung von Produktsicherheitsdaten:
Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung rechtlicher Verpflichtungen als Hersteller von Medizinprodukten oder Arzneimitteln ist Art. 6 Abs.1 lit. c, Art. 9 Abs. 2 lit. i DSGVO in Verbindung mit den Pflichten zur Überwachung nach dem Inverkehrbringen nach dem Medizinproduktegesetz und der Medizinprodukterichtlinie (geregelt ab dem 26. Mai 2021 in Kapitel VII der neuen Medizinprodukteverordnung (EU) 2017/745) und/oder dem Arzneimittelgesetz.

ÄNDERUNGEN DER DATENSCHUTZRICHTLINIE

Nur anwendbar, wenn Sie myoncare Tools für Kostenerstattungen nutzen.
Das **myoncare-Portal** unterstützt Sie bei der Einleitung Ihrer Standardverfahren zur Erstattung der Gesundheitsleistungen, die Sie Ihren Patienten über die **myoncare-App** bereitgestellt haben. Um den

Erstattungsprozess zu ermöglichen, unterstützt das **myoncare-Portal** die Erfassung der persönlichen (gesundheitsbezogenen) Daten Ihrer Patienten aus dem **myoncare-Portal**, um die Übermittlung dieser Daten an die Kostenträger des Patienten im Rahmen der Standard-Erstattungsprozesse zu erleichtern (entweder Ihre Kassenärztliche Vereinigung und/oder die Krankenversicherung des Patienten). Sie sind der Datenverantwortliche für die Erstattungsdaten und verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen für die Verarbeitung der personenbezogenen Daten Ihrer Patienten im Erstattungsprozess. ONCARE agiert als Datenverarbeiter auf der Grundlage der Datenverarbeitungsvereinbarung mit dem **Leistungserbringer**.

Arten von Daten: Name des Patienten, Diagnose, Indikationen, Behandlung, Behandlungsdauer, andere Daten, die für die Verwaltung der Erstattung erforderlich sind.

Verarbeitung von Erstattungsdaten: Sie als Verantwortlicher übermitteln die für die Erstattung erforderlichen Behandlungsdaten des Patienten an den Kostenträger (entweder Ihre Krankenkasse und/oder die Krankenkasse des Patienten) und der Kostenträger verarbeitet die Erstattungsdaten, um Ihnen die Erstattung zu erstatten.

Begründung für die Verarbeitung von Erstattungsdaten: Die Verarbeitung der Erstattungsdaten erfolgt auf Grundlage der §§ 295, 301 SGB V. Die Verarbeitung der Daten durch ONCARE für Sie erfolgt ebenfalls auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

WELCHE TECHNOLOGIE WIRD VOM MYONCARE PORTAL UND DER MYONCARE APP VERWENDET?

Das **myoncare Portal** funktioniert als webbasiertes Tool, für das Sie eine funktionierende Internetverbindung und eine aktuelle Version des Internetbrowsers Chrome, Firefox oder Safari benötigen.

E-Mail-Dienst

Wir verwenden Brevo (bereitgestellt von der Sendinblue GmbH, mit Sitz in der Köpenicker Straße 126, 10179 Berlin) und Sendgrid (bereitgestellt von Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Diese E-Mail-Dienste können verwendet werden, um den Versand von E-Mails zu organisieren. Sendgrid wird verwendet, um Bestätigungs-E-Mails, Transaktionsbestätigungen und E-Mails mit wichtigen Informationen zu Anfragen zu senden. Die von Ihnen zum Zwecke des Empfangs von E-Mails eingegebenen Daten werden auf den Servern von Sendgrid gespeichert. Wenn wir in Ihrem Namen E-Mails über SendGrid versenden, verwenden wir eine SSL-gesicherte Verbindung.

Die E-Mail-Kommunikation wird für die folgenden Aufgaben verwendet:

- Erstmaliges Einloggen in die Webanwendung;
- Zurücksetzen des Passworts für die Webanwendung;
- Erstellen Sie ein Konto für die Patientenanwendung;
- Zurücksetzen des Passworts für die Patientenanwendung;
- Erstellung und Versand eines Berichts;
- Ersetzen Sie Push-Benachrichtigungen durch E-Mails für **PWA** (Progressive Web App) in den folgenden Fällen:

(i) Wenn ein Careplan innerhalb eines Tages endet;
(ii) wenn Medikamente zugewiesen wurden;
(iii) wenn die Datenschutzrichtlinie aktualisiert wurde;
iv) wenn ein Termin an Patienten und Ärzte gesendet wird, insbesondere für die Terminart "Videoanruf";
(v) Alle Informationen, die sich auf eine **Caretask** beziehen oder wenn ein **Leistungserbringer** einen Caretask zugewiesen hat.

Speicherdauer

Die Daten, die Sie uns zum Empfang von E-Mails zur Verfügung stellen, werden von uns gespeichert, bis Sie sich von unseren Diensten abmelden, und nach Ihrer Abmeldung sowohl von unseren Servern als auch von den Servern von Sendgrid gelöscht.

Brevo (Datenschutzerklärung):
Datenschutzerklärung - Schutz personenbezogener Daten | Brevo

SendGrid (englisch)
https://sendgrid.com/resource/general-data-protection-regulation-2/

Matomo

Dabei handelt es sich um ein Open-Source-Web-Analyse-Tool. Matomo (bereitgestellt von InnoCraft Ltd.,

Neuseeland) überträgt keine Daten an Server, die außerhalb der Kontrolle von ONCARE liegen. Matomo ist zunächst deaktiviert, wenn Sie unsere Dienste nutzen. Nur wenn Sie damit einverstanden sind, wird Ihr Nutzerverhalten anonymisiert erfasst. Wenn diese deaktiviert ist, wird ein "dauerhaftes Cookie" gespeichert, sofern Ihre Browsereinstellungen dies zulassen. Dieses Cookie signalisiert Matomo, dass Sie nicht möchten, dass Ihr Browser aufgezeichnet wird.

Die durch das Cookie gesammelten Nutzungsinformationen werden an unsere Server übertragen und dort gespeichert, damit wir das Nutzerverhalten analysieren können.
Die vom Cookie erzeugten Informationen über Ihre Nutzung sind:
- Betriebssystem des Benutzers;
- Geolokalisierung des Benutzers;
-Browser;
-Rolle;
-IP-Adresse;
- Websites, die über das Web / PWA besucht werden (weitere Informationen finden Sie im Abschnitt über PWA in dieser Datenschutzrichtlinie);
- Schaltflächen, die der Benutzer im **myoncare-Portal**, in der **myoncare-App** und in der **myoncare-PWA** anklickt.
Die durch das Cookie erzeugten Informationen werden nicht an Dritte weitergegeben.

Sie können die Verwendung von Cookies ablehnen, indem Sie die entsprechenden Einstellungen in Ihrem Browser vornehmen. Bitte beachten Sie jedoch, dass Sie in diesem Fall möglicherweise nicht alle Funktionen nutzen können. Weitere Informationen finden Sie unter: https://matomo.org/privacy-policy/

Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Nutzer ist Art. 6 Abs. 1 Satz 1 lit. a DSGVO. Die Verarbeitung personenbezogener Daten der Nutzer ermöglicht uns eine Analyse des Nutzungsverhaltens. Durch die Auswertung der gewonnenen Daten sind wir in der Lage, Informationen über die Nutzung der einzelnen Komponenten unserer Dienste zusammenzustellen. Dies hilft uns, unsere Dienste und deren Usability kontinuierlich zu verbessern.

Wir verarbeiten und speichern personenbezogene Daten nur so lange, wie es zur Erfüllung des beabsichtigten Zwecks erforderlich ist.

SICHERE ÜBERTRAGUNG PERSONENBEZOGENER DATEN

Wir setzen angemessene technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre bei uns gespeicherten personenbezogenen Daten optimal gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Die Sicherheitsstufen werden in Zusammenarbeit mit Sicherheitsexperten kontinuierlich überprüft und an neue Sicherheitsstandards angepasst.

Der Datenaustausch vom und zum Portal sowie von und zur App erfolgt verschlüsselt. Wir bieten SSL als Verschlüsselungsprotokoll für eine sichere Datenübertragung an. Auch der Datenaustausch ist durchgehend verschlüsselt und erfolgt mit Pseudoschlüsseln.

DATENÜBERTRAGUNGEN / OFFENLEGUNG AN DRITTE

Eine Weitergabe Ihrer personenbezogenen Daten an Dritte erfolgt nur im Rahmen der gesetzlichen Bestimmungen oder auf Grundlage Ihrer Einwilligung. In allen anderen Fällen werden die Informationen nicht an Dritte weitergegeben, es sei denn, wir sind aufgrund zwingender gesetzlicher Vorschriften dazu verpflichtet (Weitergabe an externe Stellen, einschließlich Aufsichts- oder Strafverfolgungsbehörden).

Jede Übertragung personenbezogener Daten wird während der Übertragung verschlüsselt.

Die Informationen, wie wir mit den persönlichen (Gesundheits-) Daten Ihrer Patienten, die die **myoncare App** nutzen, umgehen, sind in einer separaten **Datenschutzerklärung** für die **myoncare Patienten-App** zusammengefasst. Sie finden die **Datenschutzerklärung für Patienten** hier. Bitte lesen Sie auch diese Datenschutzerklärung für Patienten sorgfältig durch. Für einen Teil der Verarbeitung von Patientendaten sind Sie der Datenbeauftragte und verantwortlich für die Einhaltung des Datenschutzes (z.B. Übermittlung von Behandlungsdaten an den Patienten).

ALLGEMEINE INFORMATIONEN ZUR EINWILLIGUNG IN DIE DATENVERARBEITUNG

Ihre Einwilligung stellt auch eine Einwilligung in die datenschutzrechtliche Datenverarbeitung dar. Bevor Sie Ihre Einwilligung erteilen, informieren wir Sie über den Zweck der Datenverarbeitung und Ihr Widerspruchsrecht.
Wenn sich die Einwilligung auch auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht, wird das **myoncare-Portal** Sie im Rahmen des Einwilligungsverfahrens ausdrücklich darüber informieren.
Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darf nur erfolgen, wenn dies aufgrund gesetzlicher Bestimmungen erforderlich ist und kein Grund zur Annahme besteht, dass Ihre berechtigten Interessen der Verarbeitung dieser personenbezogenen Daten entgegenstehen oder Sie Ihre Einwilligung in die Verarbeitung dieser personenbezogenen Daten gemäß Art. 9 Abs. 2 DSGVO gegeben haben.
Für die Datenverarbeitung, für die Ihre Einwilligung erforderlich ist (wie in dieser **Datenschutzerklärung** erläutert), wird die Einwilligung im Rahmen des Registrierungsprozesses eingeholt. Nach erfolgreicher Registrierung können die Einwilligungen in den Kontoeinstellungen des **myoncare-Portals** verwaltet werden. Darüber hinaus wird ONCARE Sie bitten, einem Auftragsverarbeitungsvertrag für die von ONCARE unter Ihrer Verantwortung als Verantwortlicher verarbeiteten Daten zuzustimmen.

DATENEMPFÄNGER / KATEGORIEN VON EMPFÄNGERN

In unserer Organisation stellen wir sicher, dass nur diejenigen Personen berechtigt sind, personenbezogene Daten zu verarbeiten, die zur Erfüllung ihrer vertraglichen und gesetzlichen Pflichten dazu verpflichtet sind.

In bestimmten Fällen unterstützen Dienstleister unsere Fachabteilungen bei der Erfüllung ihrer Aufgaben. Mit allen Dienstleistern, die Auftragsverarbeiter für personenbezogene Daten sind, wurden die erforderlichen Datenschutzvereinbarungen abgeschlossen. Bei diesen Dienstleistern handelt es sich um Google (Google Firebase), Anbieter von Cloud-Speichern und Support-Dienstleistern.

Google Firebase ist eine „NoSQL-Datenbank“, die die Synchronisierung zwischen dem myoncare Portal Ihres Leistungserbringers und der myoncare App ermöglicht. NoSQL definiert einen Mechanismus zum Speichern von Daten, der nicht nur in tabellarischen Beziehungen modelliert wird, indem es eine einfachere "horizontale" Skalierung im Vergleich zu tabellarischen/relationalen Datenbankmanagementsystemen in einem Cluster von Maschinen ermöglicht.

Zu diesem Zweck wird ein Pseudokey des **myoncare-Portals** und der **myoncare-App** zusammen mit dem entsprechenden Behandlungsplan in Google Firebase gespeichert. Die Datenübertragung erfolgt für ONCARE und seine Dienstleister pseudonymisiert, was bedeutet, dass ONCARE und seine Dienstleister keine Beziehung zu Ihnen als betroffene Person aufbauen können. Dies wird erreicht, indem die Daten während der Übertragung verschlüsselt werden und anstelle von persönlichen Identifikatoren wie Namen oder E-Mail-Adressen Pseudoschlüssel zur Nachverfolgung dieser Übertragungen verwendet werden. Die Re-Identifizierung erfolgt, sobald die personenbezogenen Daten das Patienten-Konto in der **myoncare-App** oder Ihr Konto im **myoncare-Portal** nach der Verifizierung durch spezifische Tokens erreicht haben.

Unsere Cloud-Speicheranbieter bieten Cloud-Speicher an, in dem der Firebase-Manager, der die Firebase-URLs für das **myoncare-Portal** verwaltet, gespeichert wird. Darüber hinaus stellen diese Dienstanbieter die isolierte Serverdomäne des **myoncare-Portals** bereit, in der sowohl Ihre persönlichen Daten als auch die Ihrer Patienten gespeichert werden. Es hostet auch den Video- und Dateiverwaltungsdienst von myoncare, der verschlüsselte Videokonferenzen und den Datenaustausch zwischen Ihnen und Ihrem Patienten ermöglicht. Der Zugriff auf Ihre persönlichen Daten durch Sie und Ihren Patienten wird durch das Versenden spezifischer Token gewährleistet. Diese personenbezogenen Daten werden während der Übertragung verschlüsselt und für ONCARE und seine Dienstleister während der Übertragung und im Ruhezustand pseudonymisiert. Die Leistungserbringer von ONCARE haben zu keinem Zeitpunkt Zugriff auf diese personenbezogenen Daten.

Des Weiteren setzen wir Dienstleister ein, um Serviceanfragen (Support-Dienstleister) bezüglich der

Nutzung des Accounts zu bearbeiten, z.B. wenn Sie Ihr Passwort vergessen haben, Ihre gespeicherte E-Mail-Adresse ändern möchten etc. Mit diesen Dienstleistern wurden die erforderlichen Auftragsverarbeitungsverträge abgeschlossen; darüber hinaus wurden die mit der Bearbeitung von Serviceanfragen betrauten Mitarbeiter entsprechend geschult. Nach Erhalt Ihrer Serviceanfrage wird ihr eine Ticketnummer zugewiesen.
Handelt es sich um eine Serviceanfrage bezüglich Ihrer Account-Nutzung, werden die relevanten Informationen, die Sie uns bei der Kontaktaufnahme zur Verfügung gestellt haben, an einen der autorisierten Mitarbeiter des externen Dienstes weitergeleitet. Er wird sich dann mit Ihnen in Verbindung setzen.
Andernfalls bleiben sie weiterhin von speziell zugelassenen ONCARE-Mitarbeitern verarbeitet, wie unter "VERARBEITUNG VON OPERATIVEN DATEN" beschrieben.

Über unsere Support-Dienstleister nutzen wir das Tool RepairCode, auch bekannt als Digital Twin Code. Dies ist eine Customer-Experience-Plattform zur Bearbeitung externer Rückmeldungen mit der Möglichkeit, Support-Tickets zu erstellen. Hier finden Sie die Datenschutzrichtlinie: https://app.repaircode.de/?main=main-client – Rechtliches/privacy.

Schlussendlich zeigen wir Ihnen Inhalte von Instagram (Anbieter: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland) ein (z. B. Bilder, Videos oder Beiträge). Wenn Sie auf einen verlinkten Instagrambeitrag klicken, werden Sie auf Instagram weitergeleitet. Dabei können von Instagram Cookies gesetzt und Nutzerdaten verarbeitet werden.

Wenn Sie eine Seite mit verlinkten Instagram-Beitrag aufrufen, kann Ihr Browser automatisch eine Verbindung zu den Servern von Instagram herstellen. Instagram erhält dadurch die Information, dass Sie unsere Website besucht haben, selbst wenn Sie kein Instagram-Konto besitzen oder nicht eingeloggt sind. Falls Sie eingeloggt sind, kann Instagram den Besuch Ihrem Benutzerkonto zuordnen.

Datenschutzerklärung:
https://privacycenter.instagram.com/policy

ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Zur Erbringung unserer Dienste können wir Dienstleister in Anspruch nehmen, die außerhalb der Europäischen Union ansässig sind. Wenn die Daten in ein Drittland übertragen werden, in welchem der Schutz für personenbezogene Daten als nicht angemessen beurteilt wurde, stellen wir sicher, dass angemessene Maßnahmen in Übereinstimmung mit nationalem und europäischem Recht getroffen werden und das – falls erforderlich – entsprechende Standardvertragsklauseln zwischen den verarbeitenden Parteien vereinbart wurden.

Personenbezogene Daten, die vom **myoncare-Portal** oder der **myoncare-App** erfasst werden, werden nicht in den App-Stores gespeichert. Eine Übermittlung personenbezogener Daten in Drittländer (außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums) erfolgt nur, wenn dies zur Erfüllung der vertraglichen Verpflichtung erforderlich ist, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben.

Die Synchronisierung des **myoncare-Portals** mit der **myoncare-App** erfolgt mithilfe von Google Firebase. Die Server von Google Firebase werden in der Europäischen Union gehostet. Gleichwohl ist nach den Allgemeinen Geschäftsbedingungen von Google Firebase eine vorübergehende Datenübermittlung in Länder möglich, in denen Google und verwandte Dienstleister Niederlassungen unterhalten; Bei bestimmten Google Firebase-Diensten erfolgt eine Datenübermittlung nur in die USA, es sei denn, die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Unbefugte Zugriffe auf Ihre Daten werden durch Ende-zu-Ende-Verschlüsselung und sichere Zugriffstoken verhindert. Unsere Online-Server werden in Deutschland gehostet. Zu Analysezwecken enthalten die mit SendGrid versendeten E-Mails ein sogenanntes "Zählpixel", das sich beim Öffnen der E-Mail mit den Servern von Sendgrid verbindet. Damit kann festgestellt werden, ob eine E-Mail-Nachricht geöffnet wurde.

Rechtsgrundlage
Die Datenverarbeitung erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Diese

Einwilligung können Sie jederzeit widerrufen. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitungsvorgänge bleibt vom Widerruf unberührt.

Bitte beachten Sie, dass Ihre Daten in der Regel von uns an einen Server von SendGrid in den USA übermittelt und dort gespeichert werden. Wir haben mit Sendgrid einen Vertrag abgeschlossen, der die EU-Standardvertragsklauseln enthält. Dadurch wird sichergestellt, dass ein Schutzniveau besteht, das mit dem der EU vergleichbar ist.

Wir binden Inhalte von Instagram ein, die von der Meta Platforms Ireland Ltd. bereitgestellt werden. Wenn Sie einen verlinkten Instagram-Beitrag anklicken, kann es sein, dass personenbezogene Daten (z. B. IP-Adresse, Browser-Informationen, Interaktionen) an Meta Platforms Inc. in die USA oder andere Drittländer übermittelt werden.
Meta ist unter dem EU-U.S. Data Privacy Framework (DPF) zertifiziert, wodurch für die Übermittlung in die USA ein angemessenes Datenschutzniveau anerkannt ist. Dennoch können auch Daten in Länder übertragen werden, für die kein Angemessenheitsbeschluss der Europäischen Kommission besteht. In solchen Fällen können zusätzliche Schutzmaßnahmen erforderlich sein, deren Wirksamkeit jedoch nicht immer garantiert werden kann.

Zur Verarbeitung von Aktivitätsdaten werden auf dem mobilen Gerät des **App-Nutzers** Schnittstellen zu Google Cloud-Diensten (im Fall von GoogleFit) oder zu AppleHealth oder Withings verwendet. Die **myoncare-Tools** nutzen diese Schnittstellen, die von Google, Apple und Withings bereitgestellt werden, um Aktivitätsdaten von den verbundenen Gesundheits-Apps anzufordern. Die von den **myoncare-Tools** gesendete Anfrage enthält keine personenbezogenen Daten. Personenbezogene Daten werden den **myoncare Tools** über diese Schnittstellen zur Verfügung gestellt.

DAUER DER SPEICHERUNG PERSONENBEZOGENER DATEN

Wir bewahren Ihre personenbezogenen Daten so lange auf, wie sie für den Zweck, für den sie verarbeitet werden, erforderlich sind. Bitte beachten Sie, dass zahlreiche Aufbewahrungsfristen die weitere Speicherung personenbezogener Daten erfordern. Dies gilt insbesondere für handels- oder steuerrechtliche Aufbewahrungspflichten.

Bitte beachten Sie, dass ONCARE auch Aufbewahrungspflichten unterliegt, die aufgrund der gesetzlichen Bestimmungen vertraglich mit Ihnen vereinbart werden. Darüber hinaus gelten aufgrund der Klassifizierung und gegebenenfalls Ihrer Nutzung des **myoncare-Portals** und der **myoncare-App** als Medizinprodukt bestimmte Aufbewahrungsfristen für das Portal, die sich aus dem Medizinproduktegesetz ergeben. Sofern keine anderweitigen Aufbewahrungspflichten bestehen, werden die personenbezogenen Daten routinemäßig gelöscht, sobald der Zweck erreicht ist.

Darüber hinaus können wir personenbezogene Daten aufbewahren, wenn Sie uns Ihre Einwilligung dazu erteilt haben oder wenn es zu einem Rechtsstreit kommt und wir innerhalb der gesetzlichen Verjährungsfristen, die bis zu 30 Jahre betragen können, Beweismittel verwenden; Die regelmäßige Verjährungsfrist beträgt drei Jahre.

IHRE RECHTE ALS BETROFFENE PERSON

Für die Begründung, Durchführung und Beendigung des Vertragsverhältnisses und die Erfüllung der damit verbundenen vertraglichen und gesetzlichen Pflichten sind verschiedene personenbezogene Daten erforderlich. Gleiches gilt für die Nutzung unseres **myoncare Portals** und die verschiedenen Funktionen, die es bietet.

In bestimmten Fällen müssen personenbezogene Daten auch gemäß den gesetzlichen Bestimmungen erhoben oder zur Verfügung gestellt werden. Bitte beachten Sie, dass es ohne die Bereitstellung dieser personenbezogenen Daten nicht möglich ist, Ihre Anfrage zu bearbeiten oder die zugrundeliegende vertragliche Verpflichtung zu erfüllen.

AUTOMATISIERTE ENTSCHEIDUNGEN IN EINZELFÄLLEN

Wir verwenden keine rein automatisierte Verarbeitung, um Entscheidungen zu treffen.

IHRE RECHTE ALS BETROFFENE PERSON

Wir möchten Sie über Ihre Rechte als betroffene Person informieren. Diese Rechte sind in den Artikeln 15 bis 22 DSGVO festgelegt und umfassen:

Recht auf Auskunft (Art. 15 DSGVO): Sie haben das Recht, Auskunft darüber zu verlangen, ob und wie Ihre personenbezogenen Daten verarbeitet werden, einschließlich Informationen über die Verarbeitungszwecke, Empfänger, Speicherdauer sowie Ihre Rechte auf Berichtigung, Löschung und Widerspruch. Sie haben auch das Recht, eine Kopie aller personenbezogenen Daten zu erhalten, die wir über Sie gespeichert haben.

Recht auf Löschung / Recht auf Vergessenwerden (Art. 17 DSGVO): Sie können von uns verlangen, dass Ihre von uns erhobenen und verarbeiteten personenbezogenen Daten unverzüglich gelöscht werden. In diesem Fall werden wir Sie bitten, das **myoncare Portal** von Ihrem Computer zu löschen. Bitte beachten Sie jedoch, dass wir Ihre personenbezogenen Daten erst nach Ablauf der gesetzlichen Aufbewahrungsfristen löschen können.

Recht auf Berichtigung (Art. 16 DSGVO): Sie können von uns verlangen, dass wir unrichtige personenbezogene Daten, die Sie betreffen, aktualisieren oder korrigieren oder unvollständige personenbezogene Daten vervollständigen.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO): Grundsätzlich können Sie von uns verlangen, dass wir Ihnen personenbezogene Daten, die Sie uns bereitgestellt haben und die aufgrund Ihrer Einwilligung oder der Durchführung eines Vertrages mit Ihnen automatisiert verarbeitet werden, in maschinenlesbarer Form zur Verfügung stellen, damit sie zu einem Ersatzdienstleister "portiert" werden können.

Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO): Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn die Richtigkeit der Daten bestritten wird, die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden oder ein Widerspruch gegen die Verarbeitung geprüft wird.

Recht auf Widerspruch gegen die Datenverarbeitung (Art. 21 DSGVO): Sie haben das Recht, der Verwendung Ihrer personenbezogenen Daten durch uns zu widersprechen und Ihre Einwilligung jederzeit zu widerrufen, wenn wir Ihre personenbezogenen Daten auf der Grundlage Ihrer Einwilligung verarbeiten. Wir werden unsere Dienstleistungen auch dann weiterhin erbringen, wenn sie nicht von einer widerrufenen Einwilligung abhängig sind.
Um diese Rechte auszuüben, kontaktieren Sie uns bitte unter: privacy@myoncare.com. Widerspruch und Widerruf der Einwilligung sind in Textform gegenüber privacy@myoncare.com .
Wir verlangen von Ihnen einen ausreichenden Nachweis Ihrer Identität, um sicherzustellen, dass Ihre Rechte geschützt sind und dass Ihre personenbezogenen Daten nur an Sie und nicht an Dritte weitergegeben werden.

Bitte kontaktieren Sie uns auch jederzeit unter privacy@myoncare.com wenn Sie Fragen zur Datenverarbeitung in unserem Unternehmen haben oder wenn Sie Ihre Einwilligung widerrufen möchten. Sie haben auch das Recht, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

DATENSCHUTZBEAUFTRAGTER

Unseren Datenschutzbeauftragten für alle Fragen zum Datenschutz erreichen Sie unter privacy@myoncare.com.

ÄNDERUNGEN DER DATENSCHUTZRICHTLINIE

Wir behalten uns ausdrücklich das Recht vor, diese **Datenschutzerklärung** in Zukunft nach eigenem Ermessen zu ändern. Änderungen oder Ergänzungen können beispielsweise notwendig sein, um gesetzlichen Anforderungen zu entsprechen, technische und wirtschaftliche Entwicklungen zu berücksichtigen oder den Interessen der **App**- oder **Portal-Nutzer** gerecht zu werden.

Änderungen sind jederzeit möglich und werden Ihnen in geeigneter Weise und innerhalb eines angemessenen Zeitrahmens vor ihrem Inkrafttreten mitgeteilt (z. B. durch Veröffentlichung einer überarbeiteten **Datenschutzerklärung** beim Login oder durch Vorankündigung wesentlicher Änderungen).

ONCARE GmbH

Postanschrift

Balanstraße 71a

81541 München, Germany

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Kontaktdaten des Datenschutzbeauftragten

privacy@myoncare.com

Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.

Zuletzt aktualisiert am 20. Februar 2025.

* * * *

U.S. DATENSCHUTZERKLÄRUNG

Willkommen bei myoncare, dem digitalen Gesundheitsportal für eine effiziente und bedarfsgerechte Patientenversorgung.
Für uns bei der Oncare GmbH (im Folgenden „**ONCARE**“ oder „**wir**“, „**uns**“, „**unser**“) ist der Schutz Ihrer Privatsphäre und aller Sie betreffenden personenbezogenen Daten während der Nutzung des myoncare-Portals von großer Bedeutung. Wir sind uns der Verantwortung bewusst, die sich aus der Bereitstellung und Speicherung Ihrer personenbezogenen Daten im myoncare Portal ergibt. Daher sind unsere Technologiesysteme, die für die myoncare-Dienste verwendet werden, nach höchsten Standards eingerichtet und die rechtmäßige Verarbeitung der Daten steht im Mittelpunkt unseres ethischen Verständnisses als Unternehmen.

Wir verarbeiten Ihre personenbezogenen Daten in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen zum Schutz personenbezogener Daten. In dieser Datenschutzerklärung erfahren Sie, warum und wie ONCARE Ihre personenbezogenen Daten verarbeitet, die wir von Ihnen erheben oder die Sie uns zur Verfügung stellen, wenn Sie sich für die Nutzung des myoncare-Portals entscheiden. Insbesondere finden Sie eine Beschreibung der von uns erhobenen und verarbeiteten personenbezogenen Daten sowie des Zwecks und der Grundlage, auf der wir die personenbezogenen Daten verarbeiten, und der Ihnen zustehenden Rechte.

Alle Informationen, die wir besitzen und die von Ihren Leistungserbringern bereitgestellt werden, sind **geschützte Gesundheitsinformationen (PHI)** und/oder andere medizinische Informationen. Diese sind durch bestimmte Gesetze geschützt, wie z. B. dem U.S. Health Insurance Portability and Accountability Act (**HIPAA**). Wir sind gesetzlich verpflichtet, die Privatsphäre und Sicherheit geschützter Gesundheitsinformationen zu schützen. Wir sind ständig bestrebt, Gesundheitsinformationen durch administrative, physische und technische Mittel zu schützen und ansonsten die geltenden Bundes- und Landesgesetze einzuhalten.

Bitte lesen Sie die Datenschutzrichtlinie sorgfältig durch, um sicherzustellen, dass Sie jede Bestimmung verstehen. Nachdem Sie die Datenschutzrichtlinie gelesen haben, haben Sie die Möglichkeit, der Datenschutzrichtlinie zuzustimmen und in die Verarbeitung Ihrer personenbezogenen Daten, wie in der Datenschutzrichtlinie beschrieben, einzuwilligen. Wenn Sie Ihre Einwilligung erteilen, wird die Datenschutzerklärung Bestandteil des Vertrags zwischen Ihnen und ONCARE.

Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.

DEFINITIONEN

"**App-Nutzer**" bezeichnet jeden Benutzer der myoncare App (Ihre Patienten).

"**Blockchain-Technologie**" Das myoncare-System enthält eine zusätzliche dezentrale Datenbank, in der die Daten aller Anlagen gespeichert sind.

"**Careplan-Anbieter**" bezeichnet Sie oder einen anderen Dienstleister oder Dritten (z. B. Hersteller von Medizinprodukten, Pharmaunternehmen), der Pflegepläne über den myoncare Store oder andere Mittel des Datenaustauschs anderen Nutzern des Portals zur Verfügung stellt.

"**Careplan-Nutzer**" bezeichnet Sie oder einen anderen Dienstleister (Portalnutzer), der einen Pflegeplan ("Pathway") für die Behandlung seiner registrierten Patienten verwendet.

„Care Pathway“ ist ein standardisierter Behandlungsplan, der die Schritte für Diagnosen und Therapien festlegen kann. **„Caretasks“** sind spezifische Aufgaben oder Handlungen innerhalb eines Pathways, die von den beteiligten Leistungserbringern, dem Pflegepersonal oder dem Patienten selbst durchgeführt werden müssen.

"**EU-Datenschutz-Grundverordnung**". Die Datenschutz-Grundverordnung (DSGVO) ist ein europäisches Datenschutzgesetz. Die Verordnung trat am 25. Mai 2018 in Kraft und zielt darauf ab, den Datenschutz in allen Mitgliedsstaaten zu harmonisieren und den Bürgerinnen und Bürgern mehr Kontrolle über ihre

personenbezogenen Daten zu geben. Die DSGVO gilt für alle Unternehmen und Organisationen, die in der EU tätig sind oder personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig davon, ob das Unternehmen innerhalb oder außerhalb der EU ansässig ist. Die DSGVO gilt auch für Sie als US-Bürger, da ONCARE seinen Sitz in Deutschland hat.

„**Leistungserbringer**“ bezeichnet Sie oder einen anderen Arzt, eine Klinik, eine Gesundheitseinrichtung oder einen anderen Angehörigen der Gesundheitsberufe, der allein oder im Auftrag von Ihnen oder einem anderen Arzt, einer Klinik oder einer Gesundheitseinrichtung (beabsichtigter Benutzer) handelt.

"**Gesundheitsinformationen**" bezeichnet alle Informationen, einschließlich genetischer Informationen, unabhängig davon, ob sie mündlich, in irgendeiner Form oder auf einem beliebigen Datenträger aufgezeichnet wurden,
- von einem Gesundheitsdienstleister, einer Krankenkasse, einer Gesundheitsbehörde, einem Arbeitgeber, einem Lebensversicherer, einer Schule oder Universität oder einer Clearingstelle für das Gesundheitswesen verarbeitet oder übertragen werden; und
- sich auf die vergangene, gegenwärtige oder zukünftige körperliche oder geistige Gesundheit einer Person oder einen Gesundheitszustand bezieht, auch im Zusammenhang mit der medizinischen Behandlung der Person;
- die vergangene, gegenwärtige oder zukünftige Honorarvergütung für die Gesundheitsversorgung einer Person.

„Geschützte Gesundheitsinformationen“ oder **„PHI“** bezeichnet individuell identifizierbare Gesundheitsinformationen, die (i) über elektronische Medien übertragen werden; (ii) in elektronischen Medien gespeichert werden; oder (iii) in irgendeiner anderen Form oder auf einem anderen Medium übertragen oder gespeichert werden.

„**Gesetz zur Übertragbarkeit und Verantwortlichkeit der Krankenversicherung**“ (HIPAA). Der Health Insurance Portability and Accountability Act von 1996 (**HIPAA**) ist ein US-amerikanisches Bundesgesetz, das die Schaffung nationaler Standards zum Schutz sensibler Gesundheitsdaten von Patienten vor unbefugter Offenlegung ohne deren Zustimmung oder Wissen vorsieht. Die HIPAA-Anforderungen gelten für die Verwendung und Offenlegung von Gesundheitsinformationen von Einzelpersonen durch Institutionen, die dem HIPAA-Gesetz unterliegen. Diese Personen und Organisationen werden als "Covered Entities" bezeichnet.

"**myoncare App**" meint die mobile myoncare Applikation zur Verwendung durch Patienten, die die von ONCARE angebotenen Dienste nutzen möchten.

„myoncare Store“ ist die von ONCARE betriebene Plattform, die digitale Versorgungskonzepte (Behandlungspläne) für die Behandlung Ihrer registrierten Patienten über das myoncare-Portal bereitstellt.

"**myoncare Portal**" ist das myoncare-Webportal, das für die professionelle Nutzung durch Portalnutzer bestimmt ist und als Schnittstelle zwischen Portal-Nutzern und App-Nutzer dient.

"**myoncare PWA**" bezeichnet die myoncare Progressive Web App Anwendung für Patienten, die die von Oncare angebotenen Dienste über die PWA und nicht über die myoncare App nutzen möchten.

„**myoncare-Tools**“ meint die myoncare-App und das myoncare-Portal zusammen.

"**myoncare Services**" bezeichnet die Dienste, Funktionalitäten und sonstigen Angebote, die den Portalnutzern über das myoncare Portal und/oder den App-Nutzern über die myoncare App angeboten werden oder angeboten werden können.

"**Oncare**“ bedeutet ONCARE GmbH, Deutschland.

"**Portal-Benutzer**" bezeichnet Sie oder einen anderen Dienstleister, der das webbasierte myoncare Portal nutzt.

ONCARE ist ein "Geschäftspartner" im Sinne des HIPAA und erbringt Dienstleistungen sowohl für Gesundheitsdienstleister als auch für Krankenversicherungen. Diese Dienstleistungen werden für Einrichtungen erbracht, die im HIPAA-Gesetz als

„erfasste Einheiten“ bezeichnet werden; ONCARE schließt entsprechende Vereinbarungen mit diesen Institutionen ab.
Gemäß unseren Nutzungsbedingungen richtet sich unser Angebot nur an Patientinnen und Patienten ab 18 Jahren. Dementsprechend werden keine personenbezogenen Daten von Kindern und Jugendlichen unter 18 Jahren gespeichert und verarbeitet.

„**Datenschutzerklärung**“ bezeichnet diese Erklärung, die Ihnen als Nutzer des myoncare-Portals zur Verfügung gestellt wird und beschreibt, wie wir Ihre personenbezogenen Daten erfassen, verwenden und speichern und Sie über Ihre umfassenden Rechte informiert.

„**Nutzungsbedingungen**“ bezeichnet die Nutzungsbedingungen für die Nutzung des myoncare-Portals.

EINHALTUNG VON GESETZEN

Die Oncare GmbH, ein beim Amtsgericht München unter der Registernummer 219909 eingetragenes Unternehmen mit Sitz in der Balanstraße 71a, 81541 München, Deutschland, bietet und betreibt das interaktive Webportal **myoncare-Portal** (für medizinisches Fachpersonal) und die mobile Anwendung **myoncare-App** (für Patienten) als Zugang zu den **myoncare-Diensten**. Diese **Datenschutzerklärung** gilt für alle personenbezogenen Daten, die von ONCARE im Zusammenhang mit der Nutzung des **myoncare-Portals** verarbeitet werden. Für die Nutzung der **myoncare-App** durch Patienten finden Sie eine separate Datenschutzerklärung für Patienten **hier**.

ONCARE ist ein „Business Associate“ (Geschäftspartner im Sinne von **HIPAA**), der Dienstleistungen und Gesundheitspläne für Leistungserbringer bereitstellt, die im Sinne von HIPAA als „erfasste Einheiten“ bezeichnet werden; ONCARE schließt mit diesen erfassten Unternehmen Geschäftspartnervereinbarungen ab. ONCARE wird **PHI** nur in Übereinstimmung mit den Business Associate Agreements und **HIPAA** verwenden und offenlegen.

Wir sind gemäß den U.S. Gesetzt verpflichtet, Gesetz zur Einhaltung von Vorschriften, die zum Schutz der Privatsphäre und Sicherheit geschützter Gesundheitsinformationen entwickelt wurden zu folgen. Wir werden Sie unverzüglich informieren, wenn es zu einer Verletzung (sog. Datenschutzverletzung) kommt, die die Privatsphäre oder Sicherheit von (Gesundheits-)Informationen gefährdet haben könnte.

WAS SIND PERSONENBEZOGENE DATEN IM SINNE DER DSGVO?

"**Personenbezogene Daten**" bezeichnet alle Informationen, die es ermöglichen, eine natürliche Person zu identifizieren. Dazu gehören unter anderem Ihr Name, Ihr Geburtstag, Ihre Adresse, Ihre Telefonnummer, Ihre E-Mail-Adresse und Ihre IP-Adresse.

"**Gesundheitsdaten**" sind personenbezogene Daten, die sich auf die physische und psychische Gesundheit einer natürlichen Person beziehen, einschließlich der Bereitstellung von Gesundheitsdiensten, die Informationen über ihren Gesundheitszustand offenbaren.

Daten sind als "**anonym**" anzusehen, wenn kein persönlicher Bezug zu der Person/dem Nutzer hergestellt werden kann. Im Gegensatz dazu sind „**pseudonymisierte**“ Daten Daten, bei denen der Personenbezug oder persönlich identifizierbare Informationen durch einen oder mehrere künstliche Identifikatoren oder Pseudonyme ersetzt werden, die jedoch im Allgemeinen durch den Identifikatorschlüssel wieder reidentifiziert werden können (im Sinne von Art. 4 Nr. 5 DSGVO).

myoncare PWA

Eine Progressive Web App (PWA) ist eine Website, die aussieht und die Funktionalität einer mobilen App hat. PWAs wurden entwickelt, um die nativen Funktionen mobiler Geräte zu nutzen, ohne dass ein App Store erforderlich ist. Das Ziel von PWAs ist es, den Unterschied zwischen Apps und dem traditionellen Web zu kombinieren, indem die Vorteile nativer mobiler Apps in den Browser gebracht werden. Die PWA basiert auf der Technologie von "React ". "React" ist eine Open-Source-Software für PWA-Anwendungen.

Um die myoncare PWA nutzen zu können, benötigen Patienten einen Computer oder ein Smartphone und eine aktive Internetverbindung. Es ist nicht erforderlich, eine App herunterzuladen.

Einige der myoncare App-Dienste können nicht innerhalb der myoncare PWA verwendet werden, weitere Informationen finden Sie in der Beschreibung unten. Dabei handelt es sich um die folgenden Dienstleistungen oder Spezifikationen:
-Chatten Sie mit **Leistungserbringer**;
-Video;
-Sicherheits-PIN-Codes;
-Tracking von Aktivitätsdaten (z. B. über AppleHealth, GoogleFit, Withings).

Die folgenden Informationen zur **myoncare-App** gelten auch für die **myoncare PWA**, sofern in diesem Abschnitt nicht anders beschrieben.

WELCHE PERSONENBEZOGENEN DATEN WERDEN BEI DER NUTZUNG DER MYONCARE APP VERWENDET

Wir können die folgenden Datenkategorien über Sie bei der Nutzung der **myoncare App** verarbeiten

Operative Daten: Personenbezogene Daten, die Sie uns bei der Registrierung und dem Login in unserem **myoncare Portal**, bei der Kontaktaufnahme zu Problemen mit dem Portal oder bei sonstigen Interaktionen mit uns zum Zweck der Nutzung des Portals zur Verfügung stellen;

Behandlungsdaten: Sie erfassen personenbezogene Daten Ihrer Patienten, wie Name, Alter, Größe, Gewicht, Indikation, Krankheitssymptome und andere Informationen im Zusammenhang mit der Behandlung Ihrer Patienten im **myoncare-Portal** (z. B. sind Behandlungsdaten personenbezogene Daten Ihrer Patienten, die erfasst oder verarbeitet werden, wenn Sie über das **myoncare-Portal** mit Ihrem Patienten interagieren); Aktivitätsdaten Ihrer verbundenen Patienten werden Ihnen in Ihrem **myoncare-Portal** zur Verfügung gestellt.

Kommerzielle Store-Daten: Personenbezogene Daten, die von uns verarbeitet werden, wenn Sie den **myoncare Store** entweder als Autor eines **Behandlungsplans** oder als Käufer eines **Behandlungsplans** nutzen. Die Nutzung des **myoncare Stores** erfordert die Verarbeitung Ihres Namens und Ihrer Kontaktdaten sowie Ihrer Zahlungsdaten (Zahlungsdaten nur, wenn ein **Behandlungsplan** kostenpflichtig ist).

Aktivitätsdaten: Personenbezogene Daten, die von uns verarbeitet werden, wenn ein **App-Nutzer** die **myoncare-App** mit einer Gesundheits-App (z. B. AppleHealth, GoogleFit, Withings) verbindet. Aktivitätsinformationen Ihrer angeschlossenen Patienten stehen Ihnen innerhalb des **myoncare** Portals zur Verfügung.

Kommerzielle und nicht-kommerzielle Forschungsdaten: Wir verarbeiten Ihre personenbezogenen Daten in anonymisierter/pseudonymisierter Form, um zusammenfassende wissenschaftliche Berichte zu analysieren und zu erstellen, um Produkte, Behandlungen und wissenschaftliche Ergebnisse zu verbessern.

Produktsicherheitsdaten Personenbezogene Daten, die zur Erfüllung unserer gesetzlichen Verpflichtungen als Hersteller der **myoncare App** als Medizinprodukt verarbeitet werden. Darüber hinaus können Ihre personenbezogenen Daten als Meldender eines Vorfalls verarbeitet werden, um gesetzlichen Sicherheits- oder Vigilanzanforderungen von Medizinprodukte- oder Pharmaunternehmen zu entsprechen.

Erstattungsdaten: Personenbezogene Daten, die für den Erstattungsprozess erforderlich sind.

BLOCKCHAIN-TECHNOLOGIE

Blockchain-**Technologie** („**Blockchain**“) (Europäisches Patent Nr. 4 002 787) ist ein optionaler Dienst, der nicht verpflichtend ist. Es liegt an Ihnen, dem **Leistungserbringer**, sich für die Nutzung der Blockchain-Lösung zu entscheiden. Die **Blockchain** basiert auf der Technologie von Hyperledger Fabric. Hyperledger Fabric ist eine Open-Source-Software für Blockchain-Implementierungen auf Unternehmensebene. Es bietet eine skalierbare und sichere Plattform, die Blockchain-Projekte unterstützt.

Die **Blockchain** im myoncare-System ist eine zusätzliche Datenbank, in der Daten aus der Anwendung gespeichert werden. Alle Blockchain-Daten werden in der Bundesrepublik Deutschland gespeichert. Es handelt sich um eine private **Blockchain** („**Private Blockchain**"), die nur den Input ausgewählter, verifizierter Teilnehmer zulässt, und es ist möglich, Einträge bei Bedarf zu überschreiben, zu bearbeiten oder zu löschen.

Die **Blockchain** besteht im Allgemeinen aus digitalen Daten in einer Kette von Paketen, die „Blöcke" genannt werden und die entsprechenden Transaktionen speichern. Die Art und Weise, wie diese Blöcke miteinander verbunden sind, ist chronologisch. Der erste Block, der erstellt wird, wird als Genesis-Block bezeichnet, und jeder danach hinzugefügte Block hat einen kryptografischen Hash, der sich auf den vorherigen Block bezieht, sodass Transaktionen und Informationsänderungen auf den Genesis-Block zurückgeführt werden können. Alle Transaktionen innerhalb der Blöcke werden durch einen Blockchain-Konsensmechanismus validiert und verifiziert, um sicherzustellen, dass jede Transaktion unverändert bleibt.

Jeder Block enthält die Liste der Transaktionen, eine Uhrzeit, einen eigenen Hash und den Hash des vorherigen Blocks. Ein Hash ist eine Funktion, die digitale Daten in eine alphanumerische Kette umwandelt. In diesem Fall kann der Block nicht mehr mit den anderen synchronisiert werden. Wenn eine unbefugte Person versucht, die Daten eines einzelnen Blocks zu ändern, ändert sich auch der Hash des Blocks und die Verknüpfung zu diesem Block geht verloren. Wenn alle Knoten (Netzwerkknoten) versuchen, ihre Kopien zu synchronisieren, wird festgestellt, dass eine Kopie geändert wurde, und das Netzwerk betrachtet diesen Knoten als fehlerhaft. Dieser technische Prozess verhindert, dass Unbefugte die Inhalte der Blockchain-Kette manipulieren können.

Unsere **Blockchain** ist eine **private** Blockchain. Eine private **Blockchain** ist dezentralisiert. Dabei handelt es sich um ein sogenanntes Distributed-Ledger-System (digitales System zur Erfassung von Transaktionen), das als geschlossene Datenbank fungiert. Im Gegensatz zu öffentlichen **Blockchains**, die „unauthorisiert" sind, sind **private Blockchains** „autorisiert", da eine Autorisierung erforderlich ist, um Nutzer zu werden. Im Gegensatz zu öffentlichen **Blockchains**, die für jeden öffentlich zugänglich sind, ist der Zugang zu **privaten Blockchains** von einer Autorisierung abhängig, um Nutzer zu werden. Diese Struktur ermöglicht es, die Sicherheit und Unveränderlichkeit der **Blockchain-Technologie** zu nutzen und gleichzeitig datenschutzkonform zu sein, insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) einzuhalten. Private Blockchain-Datensätze können bearbeitet, geändert oder gelöscht werden. Eine Löschung bedeutet in diesem Zusammenhang, dass der Referenzwert auf die UUID (Universally Unique Identifier) in der Datenbank des **Leistungserbringers** gelöscht wird. Darüber hinaus wird der Hash in der Blockchain-Datenbank anonymisiert, so dass dieser Gesamtprozess konform mit der Datenschutz-Grundverordnung ist und die Rechte einer betroffenen Person gewährleistet sind (Recht auf Löschung "Recht auf Vergessenwerden", Art. 17 DSGVO).

Art der Daten, die in der Blockchain gespeichert und verarbeitet werden:

-Patienten-UUID
-Institutionen/**Leistungserbinger** UUID
-Asset-UUID
-Hash von **caretask** und Asset-Daten.
(*UUID: Universeller eindeutiger Identifikator*).

Die in der **Blockchain** gespeicherten Daten sind pseudonymisiert.
Unsere **Blockchain** ist darauf ausgelegt, den Datenschutz in Bezug auf Datenintegrität, Patientenprofile, Vermögenswerte sowie zugewiesene **Care Tasks** und Medikamente zu gewährleisten. Um mit der **Blockchain** zu kommunizieren, muss der Benutzer eine Reihe von öffentlichen und privaten Schlüsseln registrieren. Der Registrierungsprozess generiert Zertifikate, die in einer separaten Datenbank des **Leistungserbringers** und auf dem Mobiltelefon des Patienten gespeichert werden. Eine Sicherungskopie des Patientenschlüssels wird verschlüsselt in der Datenbank des **Leistungserbringers** gespeichert, auf die nur der Patient zugreifen kann.

Bei der Überprüfung der Zustimmung zum Datenschutz, falls der **Leistungserbringers** mit dem Patienten kommunizieren möchte, überprüft das System, ob der Patient der Datenschutzrichtlinie des

Leistungserbringers zugestimmt hat. Die **Blockchain** dient somit dazu, die Integrität und Verantwortlichkeit des Protokolls sicherzustellen, um zu gewährleisten, dass der Patient die Datenschutzrichtlinie akzeptiert hat.

Wenn ein **Leistungserbringer** eine neue Version einer Datenschutzrichtlinie hochlädt, wird der Hash der Datei auf der **Blockchain** gespeichert, und nachdem der Patient der Datenschutzrichtlinie zugestimmt hat, wird diese Interaktion auf der **Blockchain** gespeichert. Jedes Mal, wenn eine Kommunikation mit dem Patienten erfolgt, antwortet die **Blockchain**, indem sie den Hash mit einer Markierung vergleicht, die anzeigt, ob die Zustimmung des Patienten für die aktuelle Datenschutzrichtlinie noch gültig ist.

Im Falle einer Patientensynchronisation wird auch die Integrität des Patientenprofils durch die Blockchain sichergestellt. Der **Leistungserbringer** erkennt sofort, wenn das Patientenprofil nicht synchronisiert oder nicht mit dem Profil auf dem Mobiltelefon übereinstimmt, indem er den Hash des Patientenprofils in der **Blockchain** vergleicht. Auf diese Weise erreicht der **Leistungserbringer** eine ausreichende Aktualität in Bezug auf das Patientenprofil.

myoncare Portal:
Falls der **Leistungserbringer** sich für die Nutzung der Blockchain-Lösung entscheidet, implementiert ONCARE ein zusätzliches Tool namens „Adapter Service“, das zur Kommunikation mit der **Blockchain** verwendet wird. Die Blockchain-Instanz wird von ONCARE gehostet.

myoncare App:
Patienten können sich mit demselben Blockchain-Instanz mithilfe des Phone Manager-Tools verbinden, das ebenfalls von ONCARE gehostet wird. Dieser Service wird ebenfalls von ONCARE gehostet.

Rechtfertigung der Verarbeitung: Die Verarbeitung von Daten durch ONCARE im Auftrag des **Leistungserbringers** erfolgt auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

VERARBEITUNG VON OPERATIVEN DATEN

Falls Sie eine Kontaktperson für den Betrieb des **myoncare-Portals** an Ihrem Standort/Ihrer Praxis sind (z. B. IT-Administrator, benannter **Leistungserbringer**), können Sie uns bestimmte personenbezogene Daten zur Verfügung stellen, wenn Sie uns kontaktieren, um die Funktionen und die Nutzung des **myoncare-Portals** zu verstehen oder zu besprechen, oder im Falle einer Serviceanfrage.

Im Falle einer Serviceanfrage können auch folgende personenbezogene Daten von autorisierten ONCARE-Mitarbeitern eingesehen werden:
Ihre persönlichen Daten, die Sie uns für die Registrierung und/oder den Login zu unserem Portal zur Verfügung gestellt haben (z. B. Name, Geburtsdatum, Profilbild, Kontaktdaten).

Autorisierte ONCARE-Mitarbeiter, die zum Zwecke der Bearbeitung einer Serviceanfrage auf Ihre Datenbank zugreifen dürfen, sind vertraglich verpflichtet, alle personenbezogenen Daten streng vertraulich zu behandeln.

Wichtige Erläuterungen zu Push-Benachrichtigungen und E-Mails
Im Rahmen Ihrer Unterstützung durch myoncare möchten wir Sie darüber informieren, wie wir mit Benachrichtigungen umgehen und wichtige Informationen, die wir Ihnen zukommen lassen.

1. **Push-Benachrichtigungen**:
   - Wir senden Ihnen Push-Benachrichtigungen über unsere **myoncare-PWA** (Progressive Web App) und die **myoncare-App**, um Sie über Aufgaben, Termine und wichtige Updates zu informieren.
   - Sie haben die Möglichkeit, diese Push-Benachrichtigungen in den Einstellungen Ihrer App zu deaktivieren.
2. **E-Mail-Benachrichtigungen**:
   - Unabhängig davon, ob Sie Push-Benachrichtigungen aktiviert oder deaktiviert haben, senden wir Ihnen weiterhin wichtige Informationen und Erinnerungen per E-Mail.
   - So stellen Sie sicher, dass Sie keine wichtigen Benachrichtigungen verpassen und Ihr Support reibungslos läuft.

Warum wir das tun:

- Unser Ziel ist es, dass Sie stets über Ihre Aufgaben und wichtige Updates informiert sind, um Ihre Pflege optimal zu unterstützen.
- E-Mails sind ein zuverlässiger Weg, um sicherzustellen, dass wichtige Informationen Sie erreichen, auch wenn Push-Benachrichtigungen deaktiviert sind.

Ihre Handlungsoptionen:

- Wenn Sie keine Push-Benachrichtigungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare-App** deaktivieren
- Bitte stellen Sie sicher, dass Ihre E-Mail-Adresse korrekt und aktuell ist, um einen reibungslosen Empfang unserer Nachrichten zu gewährleisten.
- Wenn Sie keine E-Mail-Erinnerungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare-App** deaktivieren.

Speicherdauer
Die Daten, die Sie uns zum Empfang von E-Mails zur Verfügung stellen, werden von uns gespeichert, bis Sie sich von unseren Diensten abmelden, und nach Ihrer Abmeldung sowohl von unseren Servern als auch von den Servern von Sendgrid gelöscht.

Bei der Verarbeitung von Betriebsdaten handelt ONCARE als Datenbeauftragter, der für die rechtmäßige Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist.

Datenarten: E-Mail-Adresse, Geburtsdatum, Registrierungsdatum, Ihre IP-Adresse, vom Portal generierte Pseudokeys.

Die App verwendet die Google Maps API, um geografische Informationen zu verwenden. Bei der Nutzung von Google Maps werden von Google auch Daten über die Nutzung der Kartenfunktionen erhoben, verarbeitet und genutzt. Nähere Informationen über den Umfang, die Rechtsgrundlage und den Zweck der Datenverarbeitung durch Google sowie die Speicherdauer finden Sie in der Datenschutzerklärung von Google.

Zweck der Verarbeitung von Betriebsdaten: Wir verwenden die Betriebsdaten, um die Funktionalitäten des **myoncare-Portals** aufrechtzuerhalten und um Sie bei Bedarf oder auf Ihre Initiative hin direkt zu kontaktieren (z. B. bei Änderungen der Nutzungsbedingungen, notwendiger Unterstützung, technischen Problemen usw.). Darüber hinaus werden personenbezogene Daten (E-Mail-Adresse) im Rahmen der Zwei-Faktor-Authentifizierung jedes Mal verarbeitet, wenn Sie sich in das **myoncare-Portal** einloggen.

Rechtfertigung der Verarbeitung gemäß der DSGVO:
Die Verarbeitung personenbezogener Daten ist auf der Grundlage von Art. 6 Abs. 1 lit. b DSGVO für die Erfüllung des Vertrages, den Sie mit ONCARE zum Zwecke der Nutzung der **myoncare Portal** abschließen, gerechtfertigt.

IP GEOLOKALISIERUNG

IP-Geolokalisierung: Wir verwenden eine Geolokalisierungsanwendung für unsere Dienste. Wir verwenden ipapi (bereitgestellt von apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Wien, Österreich) und Geoapify (zur Verfügung gestellt von Keptago Ltd., N. Nikolaidi und T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Zypern) , um den Standort von Patientenbenutzern zu identifizieren. Wir verwenden sie, um unsere Anwendungen zu sichern und den Standort des Patientenbenutzers zu überprüfen, um sicherzustellen, dass die Nutzung unserer Dienste konform ist. Wir kombinieren die von uns gesammelten Informationen nicht mit anderen Informationen über den Benutzer, die ihn identifizieren könnten. Zu den von apilayer verarbeiteten Daten gehören die IP-Adresse des Patienten und weitere Angaben zum Standort. Rechtsgrundlage für die Nutzung ist Art. 6 Abs. 1 lit. f DSGVO. Die Daten werden gelöscht, wenn der mit ihr verbundene Zweck, für den sie erhoben wurden, nicht mehr besteht und keine gesetzliche Aufbewahrungspflicht mehr besteht. Weitere Informationen zu deren Datenschutzrichtlinien finden Sie unter https://ipapi.com/privacy/ und Datenschutzerklärung | Geoapify Standortplattform.

VERARBEITUNG VON (BEHANDLUNGS-) DATEN

Während der Nutzung des **myoncare-Portals** geben Sie persönliche (gesundheitsbezogene) Daten Ihrer Patienten in das **myoncare-Portal** ein (z. B. Bereitstellung eines individuellen Behandlungsplans, Erinnerung zur Medikamenteneinnahme usw.). Darüber hinaus können Sie und Ihre Patienten Dokumente und Dateien in das **myoncare Portal** hochladen und miteinander teilen. Darüber hinaus können Standortfunktionen generiert und implementiert werden:

- Hinzufügen eines Standorts;
- Hochladen des Logos der Website;
- Hinzufügen der Details des Standorts;
- Hochladen einer Datenschutzerklärung

Es ist möglich, weitere Einwilligungsanforderungen für den Patienten zu erstellen, für die der Patient eine Einwilligung erteilen muss, um sich mit der Website zu verbinden.

Eine hochgeladene Datenschutzerklärung wird jedem Patienten angezeigt, der sich mit der Website verbindet. Alle Einwilligungserklärungen müssen in der hochgeladenen Datenschutzerklärung dokumentiert werden. Sobald eine Datenschutzerklärung hochgeladen wurde, kann sie nur durch eine neue Version ersetzt, aber nicht gelöscht werden.
Die Dateien werden in einer Cloud-Datenbank in Deutschland gespeichert. Sie können die gemeinsame Nutzung solcher Dateien mit anderen **Portal-Benutzer** innerhalb Ihrer Einrichtung zu medizinischen Zwecken erlauben. Andere **Portal-Benutzer** haben keinen Zugriff auf diese Dateien.

Gemäß der DSGVO sind Sie als Datenbeauftragter für die Verarbeitung von Gesundheitsdaten von Patienten im Rahmen der Nutzung der myoncare-Dienste verantwortlich.

Wir verarbeiten diese personenbezogenen Daten, einschließlich der Gesundheitsdaten des Patienten, im Rahmen einer Vereinbarung mit Ihnen und in Übereinstimmung mit Ihren Anweisungen.

DSGVO-Regeln

Für die Zwecke der Nutzung der myoncare-Dienste mit Gesundheitsdaten von Patientinnen und Patienten sind Sie daher der verantwortliche Datenbeauftragte (gemäß DSGVO). Bitte verarbeiten Sie die Daten Ihrer Patienten nur, wenn Sie die erforderliche Dateneinwilligung von diesen Patienten eingeholt haben. ONCARE wird als Auftragsverarbeiter (gemäß DSGVO) gemäß dem gesonderten Auftragsverarbeitungsvertrag tätig, den wir mit Ihnen auf der Grundlage von Art. 28 DSGVO abgeschlossen haben.

VERARBEITUNG VON KOMMERZIELLEN SPEICHERDATEN

Gilt nur, wenn Sie den myoncare Store als Careplan-Nutzer nutzen.

Der **myoncare Store** ist in das **myoncare-Portal** integriert und bietet den Kauf von Behandlungsplänen an. Nach der Registrierung im **myoncare-Portal** können Sie sich mit Ihren Anmeldedaten mit dem **myoncare Store** verbinden. Sie können den **myoncare Store** nutzen, um Behandlungspläne als Nutzer zu erwerben.

Daten des careplan-Nutzers:
Die Daten des **Careplan-Nutzers**, die der **myoncare Store** während der Nutzung verarbeitet, werden zum Abschluss eines Lizenzvertrags mit dem **Careplan-Anbieter** – in diesem Fall ONCARE – und, falls eine Gebühr fällig ist, zur Abwicklung und Kontrolle des Zahlungsvorgangs zwischen dem **Careplan-Anbieter** – in diesem Fall ONCARE – und dem **Careplan-Nutzer** verarbeitet.

Arten von Daten: Name, Kontaktdaten, Bankverbindung.

Verarbeitung von kommerziellen Store-Daten: Personenbezogene Daten, die von uns bei der Nutzung des myoncare Stores verarbeitet werden, entweder im Zusammenhang mit der Autorenschaft von Behandlungsplänen oder dem Kauf von Behandlungsplänen. Darüber hinaus werden die Zahlungsdaten (falls eine Nutzungsgebühr erhoben wird) an den **Careplan-Anbieter** weitergeleitet.

DSGVO-Regeln

Rechtfertigung für die Verarbeitung kommerzieller Store-Daten: Die Rechtsgrundlage für die Verarbeitung

personenbezogener Daten ist die separate Auftragsverarbeitungsvereinbarung, die wir mit dem **Careplan-Anbieter** auf Grundlage von Art. 28 DSGVO abgeschlossen haben.

VERARBEITUNG VON AKTIVITÄTSDATEN

Gilt nur, wenn die Nutzer Ihrer verbundenen App der Datenübertragung zustimmen und diese aktivieren.

Die **myoncare-Tools** bieten **App-Nutzern** die Möglichkeit, die **myoncare-App** mit bestimmten Gesundheits-Apps (z. B. AppleHealth, GoogleFit, Withings) („**Gesundheits-App**“) zu verbinden, sofern diese vom **App-Nutzer** verwendet werden und die Verbindung vom **App-Nutzer** hergestellt wird. Wenn die Verbindung hergestellt ist, werden die von der **Gesundheits-App** gesammelten Aktivitätsdaten Ihnen zur Verfügung gestellt, um zusätzliche kontextuelle Informationen bezüglich der Aktivität des **App-Nutzers** bereitzustellen. Bitte beachten Sie, dass Aktivitätsdaten nicht von den **myoncare-Tools** validiert werden und daher nicht für diagnostische Zwecke oder als Grundlage für medizinische Entscheidungen verwendet werden sollten.

Die Verarbeitung der Aktivitätsdaten liegt in der Verantwortung Ihrer Patienten.

Datenarten: Der Typ und Umfang der übertragenen Daten hängen von der Entscheidung der **App-Nutzer** ab. Zu den Daten können unter anderem Gewicht, Größe, zurückgelegte Schritte, verbrannte Kalorien, Schlafstunden, Herzfrequenz und Blutdruck gehören.

Zweck der Verarbeitung von Aktivitätsdaten: Die Aktivitätsdaten des App-Nutzers werden Ihnen zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zur Aktivität des **App-Nutzers** bereitzustellen. Bitte beachten Sie, dass Aktivitätsdaten nicht von den **myoncare-Tools** validiert werden und daher nicht für diagnostische Zwecke oder als Grundlage für medizinische Entscheidungen verwendet werden sollten.

Begründung der Verarbeitung:
Der Datenbeauftragte ist der Patient selbst, indem er Ihnen Zugang zu seinen Aktivitätsdaten gewährt, um die geteilten Informationen zu überprüfen. Eine weitere Begründung bedarf es daher nicht.

VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

***Gilt nur, wenn Sie die Medizinproduktevariante der myoncare Tools verwenden*.**

Das **myoncare Portal** und die **myoncare App** werden als Medizinprodukt gemäß den europäischen Medizinproduktevorschriften klassifiziert und vermarktet. Als Hersteller des **myoncare-Tools** müssen wir bestimmten gesetzlichen Verpflichtungen nachkommen (z.B. Überwachung der Funktionalität des Tools, Auswertung von Vorfallberichten, die im Zusammenhang mit der Nutzung des Tools stehen könnten, Nachverfolgung von Nutzern usw.). Zusätzlich ermöglichen die **myoncare-Tools** Ihnen, personenbezogene Daten über bestimmte medizinische Geräte oder Medikamente zu erfassen, die bei der Behandlung Ihrer Patienten verwendet werden. Die Hersteller solcher Medizinprodukte oder Arzneimittel haben auch gesetzliche Verpflichtungen hinsichtlich der Marktüberwachung (z.B. Sammlung und Auswertung von Nebenwirkungsmeldungen).

ONCARE ist der Datenverantwortliche für die Verarbeitung von Produktsicherheitsdaten.

Arten von Daten: Fallberichte, personenbezogene Daten, die in einem Vorfallbericht angegeben wurden, und Ergebnisse der Bewertung, Angaben zum Meldenden.

Verarbeitung von Produktsicherheitsdaten: Wir speichern und werten alle personenbezogenen Daten im Zusammenhang mit unseren gesetzlichen Verpflichtungen als Hersteller eines Medizinprodukts aus und übermitteln diese personenbezogenen Daten (soweit möglich nach Pseudonymisierung) an zuständige Behörden, Benannte Stellen oder andere Datenbeauftragte mit Aufsichtspflichten. Darüber hinaus speichern und übertragen wir personenbezogene Daten im Zusammenhang mit medizinischen Geräten und/oder Medikamenten, wenn wir Mitteilungen von Ihnen als Meldender solcher Informationen, von Ihrem Patienten oder von Dritten (z. B. unseren Vertriebspartnern oder Importeuren der **myoncare-Tools** in Ihrem Land) erhalten, die dem Hersteller des

Produkts gemeldet werden müssen, damit dieser seinen gesetzlichen Verpflichtungen zur Produktsicherheit nachkommen kann.

DSGVO-Regeln

Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung rechtlicher Verpflichtungen als Hersteller von Medizinprodukten oder Arzneimitteln ist Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. i DSGVO in Verbindung mit den Pflichten zur Überwachung nach dem Inverkehrbringen nach dem Medizinproduktegesetz und der Medizinprodukterichtlinie (geregelt ab dem 26. Mai 2021 in Kapitel VII der neuen Medizinprodukteverordnung (EU) 2017/745) und/oder dem Arzneimittelgesetz.

WELCHE TECHNOLOGIE WIRD VOM MYONCARE PORTAL UND DER MYONCARE APP VERWENDET?

Das **myoncare Portal** funktioniert als webbasiertes Tool, für das Sie eine funktionierende Internetverbindung und eine aktuelle Version des Internetbrowsers Chrome, Firefox oder Safari benötigen.

E-Mail-Dienst

Wir verwenden Brevo (bereitgestellt von der Sendinblue GmbH, mit Sitz in der Köpenicker Straße 126, 10179 Berlin) und Sendgrid (bereitgestellt von Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Diese E-Mail-Dienste können verwendet werden, um den Versand von E-Mails zu organisieren. Sendgrid wird verwendet, um Bestätigungs-E-Mails, Transaktionsbestätigungen und E-Mails mit wichtigen Informationen zu Anfragen zu senden. Die von Ihnen zum Zwecke des Empfangs von E-Mails eingegebenen Daten werden auf den Servern von Sendgrid gespeichert. Wenn wir in Ihrem Namen E-Mails über SendGrid versenden, verwenden wir eine SSL-gesicherte Verbindung.

Die E-Mail-Kommunikation wird für die folgenden Aufgaben verwendet:

- Erstmaliges Einloggen in die Webanwendung;
- Workflow zum Zurücksetzen des Passworts für die Web-App;
- Erstellen Sie ein Konto für die Patientenanwendung;
- Workflow zum Zurücksetzen des Passworts für Patientenanwendungen;
- Erstellung und Versand eines Berichts;
-Ersetzen Sie Push-Benachrichtigungen durch E-Mails für PWA (Progressive Web App) in den folgenden Fällen:

(i) Wenn ein Careplan innerhalb eines Tages endet;
(ii) wenn Medikamente zugewiesen wurden;
(iii) wenn die Datenschutzrichtlinie aktualisiert wurde;
(iv) wenn ein Termin an Patienten und Ärzte gesendet wird, insbesondere für die Terminart "Videoanruf";
(v) alle Informationen in Bezug auf eine **Caretask** oder falls ein **Leistungserbringer** eine **Caretask** zugewiesen hat.

Brevo (Datenschutzerklärung):
Datenschutzerklärung - Schutz personenbezogener Daten | Brevo

SendGrid (Datenschutzerklärung):
SendGrid (Privacy Policy): https://sendgrid.com/resource/general-data-protection-regulation-2/

Matomo

Dabei handelt es sich um ein Open-Source-Web-Analyse-Tool. Matomo (bereitgestellt von InnoCraft Ltd., Neuseeland) überträgt keine Daten an Server, die außerhalb der Kontrolle von ONCARE liegen. Matomo ist zunächst deaktiviert, wenn Sie unsere Dienste nutzen. Nur wenn Sie damit einverstanden sind, wird Ihr Nutzerverhalten anonymisiert erfasst. Wenn diese deaktiviert ist, wird ein "dauerhaftes Cookie" gespeichert, sofern Ihre Browsereinstellungen dies zulassen. Dieses Cookie signalisiert Matomo, dass Sie nicht möchten, dass Ihr Browser aufgezeichnet wird.

Die durch den Cookie gesammelten Nutzungsinformationen werden an unsere Server übertragen und dort gespeichert, damit wir das Nutzerverhalten analysieren können.
Die vom Cookie erzeugten Informationen über Ihre Nutzung sind:
-Rolle;
- Geolokalisierung des Benutzers;

-Browser;
- Betriebssystem des Benutzers;
-IP-Adresse;
- Websites, die über das Web / PWA besucht werden (weitere Informationen finden Sie im Abschnitt über PWA in dieser Datenschutzrichtlinie);
- Schaltflächen, die der Benutzer im **myoncare-Portal**, in der **myoncare-App** und in der **myoncare-PWA** anklickt
Zeit, in der der Nutzer Inhalte verwendet hat.
Die durch den Cookie erzeugten Informationen werden nicht an Dritte weitergegeben.

Sie können die Verwendung von Cookies ablehnen, indem Sie die entsprechenden Einstellungen in Ihrem Browser vornehmen. Bitte beachten Sie jedoch, dass Sie in diesem Fall möglicherweise nicht alle Funktionen nutzen können. Weitere Informationen finden Sie unter: https://matomo.org/privacy-policy/ .

Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Nutzer ist Art. 6 Abs. 1 Satz 1 lit. a DSGVO. Die Verarbeitung personenbezogener Daten der Nutzer ermöglicht es uns, das Nutzungsverhalten zu analysieren. Durch die Auswertung der gewonnenen Daten sind wir in der Lage, Informationen über die Nutzung der einzelnen Komponenten unserer Dienste zusammenzustellen. Dies hilft uns, unsere Dienste und deren Usability kontinuierlich zu verbessern.

Wir verarbeiten und speichern personenbezogene Daten nur so lange, wie es zur Erfüllung des beabsichtigten Zwecks erforderlich ist.

SICHERE ÜBERTRAGUNG PERSONENBEZOGENER DATEN

Wir setzen angemessene technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre bei uns gespeicherten personenbezogenen Daten optimal gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Die Sicherheitsstufen werden in Zusammenarbeit mit Sicherheitsexperten kontinuierlich überprüft und an neue Sicherheitsstandards angepasst.

Der Datenaustausch vom und zum Portal sowie von und zur App erfolgt verschlüsselt. Wir bieten SSL als Verschlüsselungsprotokoll für eine sichere Datenübertragung an. Auch der Datenaustausch ist durchgehend verschlüsselt und erfolgt mit Pseudoschlüsseln.

DATENÜBERTRAGUNGEN / OFFENLEGUNG AN DRITTE

Wir werden Ihre personenbezogenen Daten nur im Rahmen der gesetzlichen Bestimmungen oder aufgrund Ihrer Einwilligung an Dritte weitergeben. In allen anderen Fällen werden die Informationen nicht an Dritte weitergegeben, es sei denn, wir sind aufgrund zwingender gesetzlicher Vorschriften dazu verpflichtet (Weitergabe an externe Stellen, einschließlich Aufsichts- oder Strafverfolgungsbehörden).

Wir geben Informationen und Daten über Sie nur weiter, wenn Gesetze einzelner Bundesstaaten oder U.S. Bundesgesetze dies verlangen; dies schließt Anfragen des Department of Health and Human Services mit ein, wenn die Behörde die Einhaltung von U.S. Bundesgesetzen überprüfen möchte.

Jede Übertragung personenbezogener Daten wird während der Übertragung verschlüsselt.

Die Informationen, wie wir mit den persönlichen (Gesundheits-) Daten Ihrer Patienten, die die **myoncare App** nutzen, umgehen, sind in einer separaten **Datenschutzerklärung** für die **myoncare Patienten-App** zusammengefasst. Sie finden die **Datenschutzerklärung für Patienten** hier. Bitte lesen Sie auch diese Datenschutzerklärung für Patienten sorgfältig durch. Für die Verarbeitung einiger Patientendaten sind Sie der Datenschutzbeauftragte und verantwortlich für die Einhaltung des Datenschutzes (z.B. Übermittlung von Behandlungsdaten an den Patienten).

ALLGEMEINE INFORMATIONEN ZUR EINWILLIGUNG

Ihre Einwilligung stellt auch eine Einwilligung in die datenschutzrechtliche Datenverarbeitung dar. Bevor wir Ihre Einwilligung erteilen, informieren wir Sie über den Zweck der Datenverarbeitung und Ihr Widerspruchsrecht.

DSGVO-Regeln

Wenn sich die Einwilligung auch auf die Verarbeitung besonderer Kategorien personenbezogener Daten

bezieht, wird das **myoncare-Portal** Sie im Rahmen des Einwilligungsverfahrens ausdrücklich darüber informieren. Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darf nur erfolgen, wenn dies aufgrund gesetzlicher Bestimmungen erforderlich ist und kein Grund zur Annahme besteht, dass Ihre berechtigten Interessen der Verarbeitung dieser personenbezogenen Daten entgegenstehen oder Sie Ihre Einwilligung in die Verarbeitung dieser personenbezogenen Daten gemäß Art. 9 Abs 2 DSGVO gegeben haben.
Für die Datenverarbeitung, für die Ihre Einwilligung erforderlich ist (wie in dieser **Datenschutzerklärung** erläutert), wird die Einwilligung im Rahmen des Registrierungsprozesses eingeholt. Nach erfolgreicher Registrierung können die Einwilligungen in den Kontoeinstellungen des **myoncare-Portals** verwaltet werden. Zusätzlich wird ONCARE Sie bitten, einer Datenverarbeitungsvereinbarung für die von ONCARE verarbeiteten Daten unter Ihrer Verantwortung als Datenverantwortlicher zuzustimmen.

DATENEMPFÄNGER / KATEGORIEN VON EMPFÄNGERN

In unserer Organisation stellen wir sicher, dass nur diejenigen Personen berechtigt sind, personenbezogene Daten zu verarbeiten, die zur Erfüllung ihrer vertraglichen und gesetzlichen Pflichten dazu verpflichtet sind.

In bestimmten Fällen unterstützen Dienstleister unsere Fachabteilungen bei der Erfüllung ihrer Aufgaben. Mit allen Dienstleistern, die Auftragsverarbeiter (im Sinne der DSGVO) für Gesundheitsinformationen / personenbezogene Daten sind, wurden die erforderlichen Datenschutzverträge abgeschlossen. Bei diesen Dienstleistern handelt es sich um Google (Google Firebase) Anbieter von Cloud-Speichern und Support-Dienstleistern.
Google Firebase ist eine „NoSQL-Datenbank“, die die Synchronisierung zwischen dem **myoncare Portal** Ihres Leistungserbringers und der **myoncare App** ermöglicht. NoSQL definiert einen Mechanismus zum Speichern von Daten, der nicht nur in tabellarischen Beziehungen modelliert wird, indem es eine einfachere "horizontale" Skalierung im Vergleich zu tabellarischen/relationalen Datenbankmanagementsystemen in einem Cluster von Maschinen ermöglicht.

Zu diesem Zweck wird ein Pseudokey des **myoncare-Portals** und der **myoncare-App** zusammen mit dem entsprechenden Behandlungsplan in Google Firebase gespeichert. Die Datenübertragung erfolgt für ONCARE und seine Dienstleister pseudonymisiert, was bedeutet, dass ONCARE und seine Dienstleister keine Beziehung zu Ihnen als betroffene Person aufbauen können. Dies wird erreicht, indem die Daten während der Übertragung verschlüsselt werden und anstelle von persönlichen Identifikatoren wie Namen oder E-Mail-Adressen Pseudoschlüssel zur Nachverfolgung dieser Übertragungen verwendet werden. Die Re-Identifizierung erfolgt, sobald die personenbezogenen Daten das Patienten-Konto in der **myoncare-App** oder Ihr Konto im **myoncare-Portal** nach der Verifizierung durch spezifische Tokens erreicht haben.

Unsere Cloud-Speicheranbieter bieten Cloud-Speicher an, in dem der Firebase-Manager, der die Firebase-URLs für das **myoncare-Portal** verwaltet, gespeichert wird. Darüber hinaus stellen diese Dienstanbieter die isolierte Serverdomäne des **myoncare-Portals** bereit, in der sowohl Ihre persönlichen Daten als auch die Ihrer Patienten gespeichert werden. Es hostet auch den Video- und Dateiverwaltungsdienst von myoncare, der verschlüsselte Videokonferenzen und den Datenaustausch zwischen Ihnen und Ihrem Patienten ermöglicht. Der Zugriff auf Ihre persönlichen Daten durch Sie und Ihren Patienten wird durch das Versenden spezifischer Token gewährleistet. Diese personenbezogenen Daten werden während der Übertragung verschlüsselt und für ONCARE und seine Dienstleister während der Übertragung und im Ruhezustand pseudonymisiert. Die Leistungserbringer von ONCARE haben zu keinem Zeitpunkt Zugriff auf diese personenbezogenen Daten.

Des Weiteren setzen wir Dienstleister ein, um Serviceanfragen (Support-Dienstleister) bezüglich der Nutzung des Accounts zu bearbeiten, z.B. wenn Sie Ihr Passwort vergessen haben, Ihre gespeicherte E-Mail-Adresse ändern möchten etc. Mit diesen Dienstleistern wurden die erforderlichen Auftragsverarbeitungsverträge abgeschlossen; Darüber hinaus wurden die mit der Bearbeitung von Serviceanfragen betrauten Mitarbeiter entsprechend geschult. Nach Erhalt Ihrer Serviceanfrage wird ihr eine Ticketnummer zugewiesen.

Handelt es sich um eine Serviceanfrage bezüglich Ihrer Account-Nutzung, werden die relevanten Informationen, die Sie uns bei der Kontaktaufnahme zur Verfügung gestellt haben, an einen der autorisierten Mitarbeiter des externen Dienstes weitergeleitet. Er wird sich dann mit Ihnen in Verbindung setzen.
Andernfalls bleiben sie weiterhin von speziell zugelassenen ONCARE-Mitarbeitern verarbeitet, wie unter "VERARBEITUNG VON BETRIEBSDATEN" beschrieben.

Über unsere Support-Dienstleister verwenden wir das Tool RepairCode, auch bekannt als Digital Twin Code, eine Customer-Experience-Plattform für den Umgang mit externem Feedback mit der Möglichkeit, Support-Tickets zu erstellen. Hier finden Sie die Datenschutzrichtlinie: https://app.repaircode.de/?main=main-client – Rechtliches/privacy.

Schlussendlich zeigen wir Ihnen Inhalte von Instagram (Anbieter: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland) ein (z. B. Bilder, Videos oder Beiträge). Wenn Sie auf einen verlinkten Instagrambeitrag klicken, werden Sie auf Instagram weitergeleitet. Dabei können von Instagram Cookies gesetzt und Nutzerdaten verarbeitet werden.

Wenn Sie eine Seite mit verlinkten Instagram-Beitrag aufrufen, kann Ihr Browser automatisch eine Verbindung zu den Servern von Instagram herstellen. Instagram erhält dadurch die Information, dass Sie unsere Website besucht haben, selbst wenn Sie kein Instagram-Konto besitzen oder nicht eingeloggt sind. Falls Sie eingeloggt sind, kann Instagram den Besuch Ihrem Benutzerkonto zuordnen.

Datenschutzerklärung:
https://privacycenter.instagram.com/policy

ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Zur Erbringung unserer Dienste können wir Dienstleister in Anspruch nehmen, die außerhalb der Europäischen Union ansässig sind. Wenn die Daten in ein Drittland übertragen werden, in welchem der Schutz für personenbezogene Daten als nicht angemessen beurteilt wurde, stellen wir sicher, dass angemessene Maßnahmen in Übereinstimmung mit nationalem und europäischem Recht getroffen werden und das – falls erforderlich – entsprechende Standardvertragsklauseln zwischen den verarbeitenden Parteien vereinbart wurden.

Personenbezogene Daten, die vom **myoncare-Portal** oder der **myoncare-App** erfasst werden, werden nicht in den App-Stores gespeichert.
Eine Übermittlung personenbezogener Daten in Drittländer (außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums) erfolgt nur, wenn dies zur Erfüllung der vertraglichen Verpflichtung erforderlich ist, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben.

Die Synchronisierung des **myoncare-Portals** mit der **myoncare-App** erfolgt mithilfe von Google Firebase. Die Server von Google Firebase werden in der Europäischen Union gehostet. Gleichwohl ist nach den Allgemeinen Geschäftsbedingungen von Google Firebase eine vorübergehende Datenübermittlung in Länder möglich, in denen Google und verwandte Dienstleister Niederlassungen unterhalten; Bei bestimmten Google Firebase-Diensten erfolgt eine Datenübermittlung nur in die USA, es sei denn, die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Unbefugter Zugriff auf Ihre Daten wird durch Ende-zu-Ende-Verschlüsselung und sichere Zugriffstoken verhindert. Unsere Server werden in Deutschland gehostet. Zu Analysezwecken enthalten die mit SendGrid versendeten E-Mails ein sogenanntes "Zählpixel", das sich beim Öffnen der E-Mail mit den Servern von Sendgrid verbindet. Damit kann festgestellt werden, ob eine E-Mail-Nachricht geöffnet wurde.

DSGVO-Regeln

Die Datenverarbeitung erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Diese Einwilligung können Sie jederzeit widerrufen. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitungsvorgänge bleibt vom Widerruf unberührt.

Bitte beachten Sie, dass Ihre Daten in der Regel von uns an einen Server von SendGrid in den USA übermittelt und dort gespeichert werden. Wir haben mit Sendgrid

einen Vertrag abgeschlossen, der die EU-Standardvertragsklauseln enthält. Dadurch wird sichergestellt, dass ein Schutzniveau besteht, das mit dem der EU vergleichbar ist.

Wir binden Inhalte von Instagram ein, die von der Meta Platforms Ireland Ltd. bereitgestellt werden. Wenn Sie einen verlinkten Instagram-Beitrag anklicken, kann es sein, dass personenbezogene Daten (z. B. IP-Adresse, Browser-Informationen, Interaktionen) an Meta Platforms Inc. in die USA oder andere Drittländer übermittelt werden.
Meta ist unter dem EU-U.S. Data Privacy Framework (DPF) zertifiziert, wodurch für die Übermittlung in die USA ein angemessenes Datenschutzniveau anerkannt ist. Dennoch können auch Daten in Länder übertragen werden, für die kein Angemessenheitsbeschluss der Europäischen Kommission besteht. In solchen Fällen können zusätzliche Schutzmaßnahmen erforderlich sein, deren Wirksamkeit jedoch nicht immer garantiert werden kann.

Zur Verarbeitung von Aktivitätsdaten werden auf dem mobilen Gerät des **App-Nutzers** Schnittstellen zu Google Cloud-Diensten (im Fall von GoogleFit) oder zu AppleHealth oder Withings verwendet. Die **myoncare-Tools** nutzen diese Schnittstellen, die von Google, Apple und Withings bereitgestellt werden, um Aktivitätsdaten von den verbundenen Gesundheits-Apps anzufordern. Die von den **myoncare-Tools** gesendete Anfrage enthält keine personenbezogenen Daten. Personenbezogene Daten werden den **myoncare-Tools** über diese Schnittstellen zur Verfügung gestellt.

DAUER DER SPEICHERUNG PERSONENBEZOGENER DATEN GEMÄSS DSGVO

Wir bewahren Ihre personenbezogenen Daten so lange auf, wie sie für den Zweck, für den sie verarbeitet werden, erforderlich sind. Bitte beachten Sie, dass zahlreiche Aufbewahrungsfristen die weitere Speicherung personenbezogener Daten erfordern. Dies gilt insbesondere für handels- oder steuerrechtliche Aufbewahrungspflichten.

Bitte beachten Sie, dass ONCARE auch Aufbewahrungspflichten unterliegt, die aufgrund der gesetzlichen Bestimmungen vertraglich mit Ihnen vereinbart werden. Darüber hinaus gelten aufgrund der Klassifizierung und gegebenenfalls Ihrer Nutzung des **myoncare-Portals** und der **myoncare-App** als Medizinprodukt bestimmte Aufbewahrungsfristen für das Portal, die sich aus dem Medizinproduktegesetz ergeben. Sofern keine anderweitigen Aufbewahrungspflichten bestehen, werden die personenbezogenen Daten routinemäßig gelöscht, sobald der Zweck erreicht ist.

Darüber hinaus können wir personenbezogene Daten aufbewahren, wenn Sie uns Ihre Einwilligung dazu erteilt haben oder wenn es zu einem Rechtsstreit kommt und wir innerhalb der gesetzlichen Verjährungsfristen, die bis zu 30 Jahre betragen können, Beweismittel verwenden; Die regelmäßige Verjährungsfrist beträgt drei Jahre.

SICHERE ÜBERTRAGUNG PERSONENBEZOGENER DATEN

Für die Begründung, Durchführung und Beendigung des Vertragsverhältnisses und die Erfüllung der damit verbundenen vertraglichen und gesetzlichen Pflichten sind verschiedene personenbezogene Daten erforderlich. Gleiches gilt für die Nutzung unserers **myoncare Portals** und die verschiedenen Funktionen, die es bietet.

AUTOMATISIERTE ENTSCHEIDUNGEN (GEMÄSS DSGVO) IM EINZELFALL

Wir verwenden keine rein automatisierte Verarbeitung, um Entscheidungen zu treffen.

IHRE RECHTE ALS BETROFFENE PERSON (GEMÄSS DSGVO)

Wir möchten Sie über Ihre Rechte als betroffene Person informieren. Diese Rechte sind in den Artikeln 15 bis 22 DSGVO festgelegt und umfassen:

Recht auf Auskunft (Art. 15 DSGVO): Sie haben das Recht, Auskunft darüber zu verlangen, ob und wie Ihre personenbezogenen Daten verarbeitet werden, einschließlich Informationen über die Verarbeitungszwecke, Empfänger, Speicherdauer und Ihre Rechte auf Berichtigung, Löschung und Widerspruch. Sie haben auch das Recht, eine Kopie aller personenbezogenen Daten zu erhalten, die wir über Sie gespeichert haben.

Recht auf Löschung / Recht auf Vergessenwerden (Art. 17 DSGVO): Sie können von uns verlangen, dass Ihre von uns erhobenen und verarbeiteten personenbezogenen Daten unverzüglich gelöscht werden. In diesem Fall werden wir Sie bitten, das **myoncare Portal** von Ihrem Computer zu löschen. Bitte beachten Sie jedoch, dass wir Ihre personenbezogenen Daten erst nach Ablauf der gesetzlichen Aufbewahrungsfristen löschen können.

Recht auf Berichtigung (Art. 16 DSGVO): Sie können von uns verlangen, dass wir unrichtige personenbezogene Daten, die Sie betreffen, aktualisieren oder korrigieren oder unvollständige personenbezogene Daten vervollständigen.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO): Grundsätzlich können Sie von uns verlangen, dass wir Ihnen personenbezogene Daten, die Sie uns zur Verfügung gestellt haben und die auf Grundlage Ihrer Einwilligung oder der Durchführung eines Vertrages mit Ihnen automatisiert verarbeitet werden, in maschinenlesbarer Form zur Verfügung stellen, damit diese zu einem Ersatzdienstleister "portiert" werden können.

Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO): Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn die Richtigkeit der Daten bestritten wird, die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden oder ein Widerspruch gegen die Verarbeitung geprüft wird.

Recht auf Widerspruch gegen die Datenverarbeitung (Art. 21 DSGVO): Sie haben das Recht, der Verwendung Ihrer personenbezogenen Daten durch uns zu widersprechen und Ihre Einwilligung jederzeit zu widerrufen, wenn wir Ihre personenbezogenen Daten auf der Grundlage Ihrer Einwilligung verarbeiten. Wir werden unsere Dienstleistungen auch dann weiterhin erbringen, wenn sie nicht von einer widerrufenen Einwilligung abhängig sind.

Um diese Rechte auszuüben, kontaktieren Sie uns bitte unter: privacy@myoncare.com mailto: privacy@myoncare.com. Widerspruch und Widerruf der Einwilligung müssen in Textform an privacy@myoncare.com erklärt werden.
Wir verlangen von Ihnen einen ausreichenden Nachweis Ihrer Identität, um sicherzustellen, dass Ihre Rechte geschützt sind und dass Ihre personenbezogenen Daten nur an Sie und nicht an Dritte weitergegeben werden.

Bitte wenden Sie sich auch jederzeit unter privacy@myoncare.com an uns, wenn Sie Fragen zur Datenverarbeitung in unserem Unternehmen haben oder Ihre Einwilligung widerrufen möchten. Sie haben auch das Recht, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

EINE BESCHWERDE EINREICHEN

Wenn Sie der Meinung sind, dass Ihre Privatsphäre von ONCARE verletzt wurde, können Sie eine Beschwerde bei uns und dem U.S. Behörde Secretary of Health and Human Services in Washington, D.C. einreichen. Für Sie entstehen keine Nachteile bei der Einreichung einer Beschwerde. Um eine Beschwerde einzureichen oder weitere Informationen zu erhalten, nutzen Sie bitte die folgenden Kontaktmöglichkeiten:
Telefon: +49 (0) 89 4445 1156

E-Mail: privacy@myoncare.com
Adresse: Balanstraße 71a
81541 München, Deutschland

Betreff: Beschwerde

Sie können eine Beschwerde bei den U.S. Ministerium für Gesundheit und Soziale Dienste einreichen indem Sie einen Brief an 200 Independence Avenue, S.W., Washington, D.C. 20201 oder rufen Sie 1-800-368-1019 (gebührenfrei) oder 1-800-537-7697 (TTD) an oder reichen Sie eine Online-Beschwerde bei https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf ein.

DATENSCHUTZBEAUFTRAGTER (GEMÄSS DSGVO)

Unser Datenschutzbeauftragter steht Ihnen bei privacy@myoncare.com für alle Fragen zum Datenschutz zur Verfügung.

ÄNDERUNGEN DER DATENSCHUTZRICHTLINIE

Wir behalten uns ausdrücklich das Recht vor, diese **Datenschutzerklärung** in Zukunft nach eigenem Ermessen zu ändern. Änderungen oder Ergänzungen können beispielsweise notwendig sein, um gesetzlichen Anforderungen zu entsprechen, technische und wirtschaftliche Entwicklungen zu berücksichtigen oder den Interessen der **App**- oder **Portal-Nutzer** gerecht zu werden.

Änderungen sind jederzeit möglich und werden Ihnen in geeigneter Weise und innerhalb eines angemessenen Zeitrahmens vor ihrem Inkrafttreten mitgeteilt (z. B. durch Veröffentlichung einer überarbeiteten **Datenschutzerklärung** beim Login oder durch Vorankündigung wesentlicher Änderungen).

Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.

ONCARE GmbH

Postanschrift

Balanstraße 71a

81541 München, Germany

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Kontaktdaten des Datenschutzbeauftragten

privacy@myoncare.com

Zuletzt aktualisiert am 20. Februar 2025

* * * *