

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 (=Plattform) 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.

Diese Datenschutzerklärung besteht aus zwei Teilen:

- Der erste Teil enthält Datenschutzregelungen für die Nutzung der myoncare Plattform innerhalb Europas auf Grundlage der Datenschutz-Grundverordnung (DSGVO).
- Die zweite Teil enthält ergänzende Bestimmungen nach den Vorgaben des US-amerikanischen Datenschutzrechts (HIPAA). Diese gelten insbesondere dann, **wenn Gesundheitsdaten durch eine US-Covered Entity verarbeitet werden oder wenn Leistungserbringer im Rahmen des US-Gesundheitssystems tätig werden** – unabhängig vom Wohnsitz der betroffenen Person.

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.

1. 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 myonclinic 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.

„myonclinic 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.

2. 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: <https://www.myoncare.com/privacy-policy>

3. 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.

Die folgenden Informationen über die **myoncare App** gilt auch für die **myoncare PWA**, sofern in diesem Abschnitt nichts anderes beschrieben ist.

4. 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: Kommerzielle Store-Daten: Personenbezogene Daten, die im Zusammenhang mit der Nutzung des myonclinic Stores verarbeitet werden – insbesondere im Zusammenhang mit der Autorenschaft, Konfiguration oder dem Erwerb von digitalen Behandlungsplänen („Pathways“). Der Store wird von der myon.clinic GmbH betrieben, einer Tochtergesellschaft der Oncare GmbH. Die Nutzung des Stores erfordert die Verarbeitung Ihres Namens, beruflicher Kontaktdaten sowie ggf. Zahlungsdaten (nur bei kostenpflichtigen Inhalten). Die Oncare GmbH verarbeitet diese Daten ausschließlich zur technischen Bereitstellung der Plattformfunktionen und nicht zu eigenen kommerziellen Zwecken.

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.

Analyse anonymisierter Nutzungsdaten zur Plattformverbesserung

Wir verarbeiten ausschließlich anonymisierte, nicht-personenbezogene technische Nutzungsdaten (z. B. aggregierte Informationen zur Nutzungshäufigkeit oder zur Systemleistung), um die Funktionalität und Benutzerfreundlichkeit des Portals weiterzuentwickeln. Diese Daten enthalten keine identifizierenden Informationen und erlauben keinen Rückschluss auf einzelne Portalnutzer. Eine Verarbeitung personenbezogener Daten von Leistungserbringern zu Forschungs- oder kommerziellen Zwecken findet nicht statt.

Daten von Geräteherstellern- oder Laboren:

Zusätzlich können im Rahmen integrierter Versorgungsprozesse personenbezogene Daten durch angebundene medizinische Gerätehersteller oder Labordienstleister verarbeitet werden, sofern diese über das myoncare Portal durch den Leistungserbringer beauftragt oder genutzt werden.

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.

5. 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 eine 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/**Leistungserbringer** 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 **Caretasks** 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 **Leistungserbringer** 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“, das 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).

6. 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 mit wichtigen 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 des **myoncare Portals** aufrechtzuerhalten und um bei Bedarf oder von Ihnen direkt initiiert 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 des **myoncare Portals** abschließen, gerechtfertigt.

7. 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](#).

8. 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. Des Weiteren 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.

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 myoncaredienste 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.

9. VERARBEITUNG VON TECHNISCHEN NUTZUNGS- UND SYSTEMDATEN

Gilt nur, wenn Sie den myonclinic Store als Careplan-Benutzer nutzen.

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

Daten des Careplan-Nutzers:

Die Daten des **Careplan-Nutzers**, die der **myonclinic 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 **myonclinic 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.

10. VERARBEITUNG VON AKTIVITÄTSDATEN

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

Die **myoncared Tools** bieten **App-Nutzern** die Möglichkeit, die **myoncared-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 **myoncared Tools** stammen und sie sollten 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 **myoncared 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.

11. VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

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

Das **myoncared Portal** und die **myoncared App** werden als Medizinprodukt gemäß den europäischen Medizinproduktevorschriften klassifiziert und vermarktet. Als Hersteller der **myoncared Tools** müssen wir bestimmten gesetzlichen Verpflichtungen nachkommen (z. B. Überwachung der Funktionalität des Tools, Auswertung von Vorfällen, die im Zusammenhang mit der Nutzung des Tools stehen könnten, Nachverfolgung von Nutzern usw.). Zusätzlich ermöglichen die **myoncared 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 Vorfalbericht 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 Medizinprodukteverordnung (geregelt ab dem 26. Mai 2021 in Kapitel VII der neuen Medizinprodukteverordnung (EU) 2017/745) und/oder dem Arzneimittelgesetz.

Ergänzung zum Haftungsabschluss für Nebenwirkungen:

Die Oncare GmbH übernimmt keine medizinische Bewertung der übermittelten Inhalte und ist nicht verpflichtet, arzneimittelrechtlich relevante Informationen wie Nebenwirkungen, Anwendungsfehler oder Produktmängel an Behörden weiterzuleiten. Diese Verantwortung liegt ausschließlich bei den behandelnden Leistungserbringer oder – sofern betroffen – bei den jeweiligen Herstellern der eingesetzten Produkte.

12. VERARBEITUNG DURCH GERÄTEHERSTELLER UND LABORDIENSTLEISTER

Wenn Sie über die Plattform medizinische Zusatzfunktionen wie integrierte Diagnostik, Vitaldatenerfassung oder Labordienstleistungen nutzen, können personenbezogene Gesundheitsdaten durch externe Drittanbieter (z. B. medizinische Gerätehersteller oder Labordienstleister) erhoben und verarbeitet werden. Dies erfolgt zur Unterstützung der medizinischen Versorgung und stets auf Grundlage einer ausdrücklichen Einwilligung oder eines Behandlungsverhältnisses.

Die Verarbeitung erfolgt entweder im Rahmen einer Auftragsverarbeitung oder – je nach Anbieter – in eigener datenschutzrechtlicher Verantwortung. Die Oncare GmbH stellt hierfür lediglich die technische Anbindung bereit, ohne Inhalte zu kontrollieren oder medizinisch zu bewerten. Weitere Informationen zur jeweiligen Datenverarbeitung erhalten Sie direkt bei dem behandelnden Leistungserbringer oder über die Datenschutzinformationen der eingebundenen Drittanbieter.

13. KOMMERZIELLE STORE-DATEN UND PATHWAY-VERWALTUNG

Das myoncare-Portal bietet registrierten Leistungserbringern (z. B. Ärzt:innen) die Möglichkeit, digitale Versorgungspfade („Pathways“) über eine Webshop-Funktionalität (z. B. in Zusammenarbeit mit myon.clinic) anzubieten, zu konfigurieren und Patient:innen individuell zuzuweisen.

Im Rahmen der Nutzung dieser Funktionalität werden personenbezogene Daten – insbesondere Gesundheitsdaten – verarbeitet, etwa Angaben zur Indikation, empfohlenen Behandlungsdauer oder Pathway-Zuordnung. Diese Datenverarbeitung dient der Individualisierung und Zuweisung medizinischer Inhalte und erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b sowie Art. 9 Abs. 2 lit. h DSGVO.

Oncare stellt die technische Infrastruktur bereit und verarbeitet die betroffenen Daten als datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, sofern die Verarbeitung zur Bereitstellung der Plattformfunktionen erforderlich ist. Die inhaltliche Auswahl und medizinische Gestaltung der Pathways obliegt jedoch ausschließlich dem jeweiligen Leistungserbringer.

Soweit eine Abrechnung oder Datenübermittlung an Dritte (z. B. Abrechnungsstellen oder Plattformpartner wie myon.clinic) erfolgt, findet eine solche Verarbeitung nur auf Grundlage entsprechender Vereinbarungen oder gesetzlicher Vorschriften statt.

12. VERARBEITUNG VON ERSTATTUNGSDATEN BEI KOSTENTRÄGERÜBERMITTLUNG

(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).

13. 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 eines Kontos für die Patientenanwendung;
- Zurücksetzen des Passworts für die Patientenanwendung;
- Erstellung und Versand eines Berichts;
- Ersetzen von Push-Benachrichtigungen durch E-Mails für **PWA** (Progressive Web App) in den folgenden Fällen:
 - Wenn ein Careplan innerhalb eines Tages endet;
 - wenn Medikamente zugewiesen wurden;
 - wenn die Datenschutzrichtlinie aktualisiert wurde;
 - wenn ein Termin an Patienten und Ärzte gesendet wird, insbesondere für die Terminart "Videoanruf";
 - 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 werden 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 dieses 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.

14. 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.

15. 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).

16. 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.

17. 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 Dienstleister 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 Ihnen 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 Datenschutzerklärung: <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) an (z. B. Bilder, Videos oder Beiträge). Wenn Sie auf einen verlinkten Instagram Beitrag klicken, werden Sie zu Instagram weitergeleitet. Dabei können von Instagram Cookies gesetzt und Nutzerdaten verarbeitet werden.

Wenn Sie eine Seite mit verlinktem 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>

18. 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 dass – 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.

19. 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.

20. 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.

21. AUTOMATISIERTE ENTSCHEIDUNGEN IN EINZELFÄLLEN

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

22. 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 einzureichen.

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.

23. DATENSCHUTZBEAUFTRAGTER

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

24. VORBEHALT DER ÄNDERUNGEN DIESER DATENSCHUTZINFORMATION

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, Deutschland

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

Kontaktdaten des Datenschutzbeauftragten privacy@myoncare.com

Sofern medizinische Inhalte oder Leistungen über den integrierten myonclinic Store bezogen oder angeboten werden, erfolgt die inhaltliche und wirtschaftliche Verantwortung durch die myon.clinic GmbH, eine Tochtergesellschaft der Oncare GmbH. Die Oncare GmbH stellt in diesem Kontext ausschließlich die technische Plattform bereit. privacy@myon.clinic

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

STAND JUNI 2025

Es folgen **ergänzende Datenschutzregelungen für Leistungserbringer**, die im Rahmen **einer HIPAA-pflichtigen Tätigkeit als Covered Entity oder im Auftrag einer solchen in den Vereinigten Staaten von Amerika** tätig werden:

Der Schutz personenbezogener Gesundheitsdaten (PHI) nach HIPAA greift ausschließlich, wenn diese Daten im Rahmen des US-Gesundheitssystems durch eine sog. Covered Entity oder einen Business Associate verarbeitet werden – unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Person. Entscheidend ist allein, dass die Verarbeitung unter den Anwendungsbereich des HIPAA fällt.

US Ergänzende Datenschutzregelungen für Leistungserbringer in den Vereinigten Staaten von Amerika (HIPAA)

1. Geltungsbereich

Diese HIPAA-Ergänzung gilt für alle Leistungserbringer, die über die ONCARE-Plattform Gesundheitsdaten (PHI – Protected Health Information) verarbeiten, speichern oder weitergeben, sofern diese Verarbeitung im Zusammenhang mit einem HIPAA-regulierten Vertragspartner („Covered Entity“) erfolgt oder ONCARE als Business Associate handelt.

2. Rollen und Verantwortlichkeiten

ONCARE fungiert in diesem Zusammenhang als Business Associate im Sinne der HIPAA Privacy Rule (45 CFR §160.103) und verpflichtet sich gegenüber der Covered Entity zur Einhaltung aller anwendbaren HIPAA-Vorschriften. Der jeweilige Leistungserbringer agiert entweder:

- als Workforce Member der Covered Entity oder
- als Subcontractor von ONCARE gemäß 45 CFR §160.103 ff.

3. Verarbeitungsrahmen

Die Nutzung der ONCARE-Plattform durch Leistungserbringer erfolgt ausschließlich auf Grundlage bestehender HIPAA-konformer Vereinbarungen mit der Covered Entity (z. B. Business Associate Agreements oder Dienstleistervereinbarungen). Die Verarbeitung umfasst insbesondere:

- Dokumentation von Behandlungsverläufen und medizinischen Leistungen,
- Kommunikation mit Patienten über HIPAA-konforme Kommunikationskanäle (Ende-zu-Ende-Verschlüsselung, TLS),
- Zugriff auf strukturierte Patientendaten zur Versorgung oder Qualitätssicherung.

4. Vertraulichkeit und Zugriffskontrolle

Leistungserbringer verpflichten sich, sämtliche PHI vertraulich zu behandeln und den Zugriff auf PHI auf das erforderliche Maß gemäß dem „Minimum Necessary Standard“ (45 CFR §164.502(b)) zu beschränken. Jeder Zugriff wird über ein rollenbasiertes Rechtekonzept verwaltet und auditierbar protokolliert.

5. Technische und organisatorische Sicherheitsmaßnahmen

Sämtliche von ONCARE implementierten Sicherheitsmaßnahmen entsprechen den Anforderungen der HIPAA Security Rule (45 CFR Part 164, Subpart C). Dazu zählen:

- AES-256-Verschlüsselung gespeicherter Daten,
- verschlüsselte Übertragung über TLS 1.3,
- Zwei-Faktor-Authentifizierung (2FA),
- regelmäßige Risikoanalysen gemäß §164.308(a)(1)(ii)(A),
- strukturierte Incident Response Prozesse.

6. Datenverarbeitung außerhalb der USA

Wenn Leistungserbringer über ONCARE auf Daten zugreifen, die außerhalb der Vereinigten Staaten verarbeitet oder gespeichert werden (z. B. Hosting in der EU), erfolgt dies ausschließlich:

- auf Basis einer HIPAA-konformen vertraglichen Absicherung (z. B. Subcontractor BAA),
- mit dokumentierter Zustimmung der Covered Entity,
- unter Einhaltung der HIPAA Security Rule und ergänzender internationaler Standards (z. B. ISO 27001, DSGVO-Prinzipien),
- und mit durchgängiger Verschlüsselung sowie Zugriffskontrolle.

7. Meldepflichten bei Datenschutzvorfällen

Leistungserbringer sind verpflichtet, ONCARE unverzüglich über jeden Vorfall zu informieren, der zu einem unautorisierten Zugriff auf PHI führen könnte („Security Incident“ oder „Breach“ gemäß 45 CFR §164.304/§164.402). ONCARE übernimmt die Koordination der gesetzlich vorgeschriebenen Meldungen an die Covered Entity und betroffene Personen.

8. Rechte der Covered Entity

Die Covered Entity behält jederzeit das Recht, im Rahmen eines Audits den Zugriff, die Verwendungsweise und die Sicherheitsmaßnahmen hinsichtlich PHI durch ONCARE und eingebundene Leistungserbringer zu prüfen. Leistungserbringer müssen die vollständige Kooperation zusichern.

9. Keine eigenständige Weitergabe

Eine Weitergabe von PHI durch den Leistungserbringer an Dritte außerhalb der Plattform (z. B. per E-Mail, externes System, Ausdruck) ist nur zulässig, wenn:

- eine dokumentierte „Authorization“ durch die betroffene Person vorliegt oder
- dies vertraglich ausdrücklich vorgesehen ist.

10. Vorrang und Auslegung

Im Falle von Widersprüchen zwischen dieser HIPAA-Ergänzung und den europäischen Datenschutzregelungen gilt stets die strengere Regelung, sofern dies im Einklang mit geltendem Recht steht. US-Bundesstaatliche Datenschutzgesetze (z. B. CCPA) bleiben unberührt und gelten ergänzend, sofern einschlägig.

11. Unterstützung bei Betroffenenrechten

Leistungserbringer unterstützen ONCARE sowie die jeweilige Covered Entity bei der Erfüllung von Rechten betroffener Personen gemäß 45 CFR §§ 164.524–528 (z. B. Auskunft, Berichtigung, Einschränkung der Weitergabe). Dies umfasst insbesondere die Mitwirkung bei:

- der Bereitstellung von Zugriffsprotokollen („Accounting of Disclosures“),
- der Korrektur fehlerhafter PHI,
- der Umsetzung von Sperrvermerken oder Einschränkungen der Nutzung.

Anfragen werden durch ONCARE koordiniert und mit einer Frist von 30 Tagen bearbeitet, mit einer möglichen Verlängerung um weitere 30 Tage bei entsprechender Mitteilung.

12. Verpflichtung zur Datenschuttschulung

Leistungserbringer sind verpflichtet, jährlich eine dokumentierte Schulung zu den datenschutzrechtlichen Vorgaben nach HIPAA und DSGVO durchzuführen.

ONCARE stellt hierfür geeignete Materialien oder E-Learning-Zugänge bereit. Die Teilnahme wird digital dokumentiert und ist auf Anforderung gegenüber der Covered Entity nachzuweisen.

13. Sekundärnutzung und Forschungsdaten

Jegliche Nutzung von PHI zu Forschungs-, Analyse- oder Marketingzwecken durch den Leistungserbringer ist unzulässig, es sei denn:

- es liegt eine dokumentierte Einwilligung („Authorization“) gemäß 45 CFR §164.508 vor,
- oder es wurde ein spezifischer, HIPAA-konformer Forschungsdatennutzungsvertrag mit ONCARE geschlossen.

Eine interne Zweitverwendung (z. B. für Qualitätssicherung) ist ausschließlich im Rahmen der Zweckbindung nach HIPAA zulässig.

14. Koordination mit DSGVO-Vorgaben

Bei gleichzeitiger Anwendbarkeit von DSGVO und HIPAA stellt ONCARE sicher, dass stets das strengere Schutzniveau gilt. Leistungserbringer verpflichten sich insbesondere:

- keine Datenübertragung außerhalb des EWR ohne entsprechende Standardvertragsklauseln oder Sub-BAA vorzunehmen,
- Betroffenenrechte aus beiden Rechtsordnungen (z. B. Recht auf Löschung nach Art. 17 DSGVO vs. Aufbewahrungspflichten nach HIPAA) im Einklang mit ONCARE zu koordinieren.

15. Ergänzende Datenschutzerfordernisse einzelner US-Bundesstaaten (USA)

Zusätzlich zu den bundesweit geltenden Regelungen gemäß dem Health Insurance Portability and Accountability Act (HIPAA) unterliegen bestimmte Datenverarbeitungen ergänzenden oder strengeren Datenschutzgesetzen einzelner US-Bundesstaaten. Dies gilt insbesondere dann, wenn betroffene Nutzer in einem dieser Bundesstaaten wohnhaft sind, unsere Dienste von dort aus nutzen oder eine Verarbeitung personenbezogener Daten durch Dienstleister oder Vertragspartner mit Sitz in diesen Bundesstaaten erfolgt.

Folgende bundesstaatliche Datenschutzgesetze können – je nach individueller Konstellation – ergänzend oder vorrangig zur Anwendung kommen:

- Kalifornien: California Consumer Privacy Act (CCPA) und California Privacy Rights Act (CPRA)
- New York: SHIELD Act
- Virginia: Virginia Consumer Data Protection Act (VCDPA)
- Colorado: Colorado Privacy Act (CPA)
- Connecticut: Data Privacy Act (CTDPA)
- Utah: Utah Consumer Privacy Act (UCPA)
- Illinois: Biometric Information Privacy Act (BIPA)
- Texas: Data Privacy and Security Act (TDPSA, in Kraft ab 01.07.2024)
- Florida: Digital Bill of Rights (FDBR)

Wir verpflichten uns, bei allen betroffenen Verarbeitungen die jeweils geltenden bundesstaatlichen Vorschriften einzuhalten und betroffenen Personen auf Anfrage umfassende Auskunft über die Anwendung dieser Rechte zu erteilen. Für bestimmte Bundesstaaten (z. B. Kalifornien) stellen wir auf Anfrage gesonderte Datenschutzhinweise zur Verfügung. Bitte kontaktieren Sie uns unter privacy@myoncare.com, wenn Sie Ihre datenschutzbezogenen Rechte nach Bundes- oder Landesrecht geltend machen möchten.

16. Keine kommerzielle Nutzung personenbezogener Daten von Portalnutzern

Personenbezogene Daten von Portalnutzern (z. B. Gesundheitsdienstleistern) werden nicht zu Forschungs-, Marketing- oder anderen kommerziellen Zwecken verarbeitet. ONCARE verarbeitet ausschließlich vollständig anonymisierte technische Nutzungsdaten (z. B. aggregierte Login-Zeitpunkte oder Systemnutzung), um die Plattform technisch zu verbessern. Diese Daten enthalten keine Informationen, die eine Identifikation einzelner Nutzer ermöglichen, und gelten nicht als „Protected Health Information“ (PHI) im Sinne der HIPAA-Datenschutzregelung.
