MYONCARE PATIENTEN APP – DATENSCHUTZERKLÄRUNG (EUROPA/USA)

STAND JUNI 2025

Willkommen bei myoncare, dem digitalen Gesundheitsportal und der mobilen App ("**App**") für eine effiziente und bedarfsgerechte Patientenversorgung und Unterstützung des betrieblichen Gesundheitsmanagements.

Diese Datenschutzerklärung gliedert sich in zwei Teile:

- Der erste Teil enthält die Datenschutzbestimmungen für die Nutzung der myoncare Plattform innerhalb Europas unter Beachtung der **EU-Datenschutz-Grundverordnung (DSGVO)**.

- Der zweite Teil enthält **ergänzende Hinweise** gemäß den Anforderungen des **Datenschutzrechts der Vereinigten Staaten von Amerika (HIPAA)**, insbesondere für Nutzer mit Wohnsitz in den USA oder bei Verarbeitung von Gesundheitsdaten durch US-amerikanische Gesundheitsdienstleister.

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 der **App** auf Sie beziehen, von großer Bedeutung und Wichtigkeit. Wir sind uns der Verantwortung bewusst, die sich aus Ihrem Vertrauen in die Bereitstellung und Speicherung Ihrer personenbezogenen (Gesundheits-)Daten in der myoncare App 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 Gesetzen. In dieser Datenschutzerklärung erfahren Sie, warum und wie **ONCARE** Ihre personenbezogenen (Gesundheits-) Daten verarbeitet, die wir von Ihnen erfassen oder die Sie uns zur Verfügung stellen, wenn Sie sich für die Nutzung der myoncare App 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.

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 der Verarbeitung Ihrer personenbezogenen (Gesundheits-)Daten, wie in der Datenschutzrichtlinie beschrieben, zuzustimmen. Wenn Sie Ihre Einwilligung geben, wird die Datenschutzerklärung Teil des Vertrages zwischen Ihnen und Oncare.
Gemäß den Nutzungsbedingungen richtet sich unser Angebot nur an Personen ab 18 Jahren. Dementsprechend werden keine personenbezogenen Daten von Kindern und Jugendlichen unter 18 Jahren gespeichert und verarbeitet.

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

1. DEFINITIONEN

"**App-Nutzer**" bezeichnet jeden Nutzer der myoncare App (Patient und/oder Mitarbeiter).

"**Blockchain**" ist im myoncare-System eine weitere Datenbank, die entsprechende Daten der Anwendung speichert.

"**Unternehmen**" bezeichnet Ihren Arbeitgeber, wenn Sie und Ihr Arbeitgeber myoncare-Tools für das betriebliche Gesundheitsmanagement des Arbeitgebers einsetzen.

"**Datendienstleister"** bezeichnet jeden Beauftragten, der von der Gesellschaft beauftragt und angewiesen wird, pseudonymisierte oder anonymisierte Mitarbeiterdaten in betrieblichen Gesundheitsmanagementprogrammen auf der Grundlage einer separaten Dienstleistungsvereinbarung mit der Gesellschaft (z. B. Datenanalyst, allgemeine Gesundheitspräventionsdienste, Datenauswertungsdienste usw.) zu sammeln, zu überprüfen und zu interpretieren, und die durch ein separates Informationsblatt an die Mitarbeiter gekennzeichnet sind.

"**Leistungserbringer**" bezeichnet Ihren Arzt, Ihre Klinik, Ihre Gesundheitseinrichtung oder andere Angehörige der Gesundheitsberufe, die allein oder im Auftrag Ihres Arztes, Ihrer Klinik oder Ihrer Gesundheitseinrichtung handeln.

"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 Aktionen innerhalb eines Pathways, die von den beteiligten Gesundheitsdienstleistern, dem Pflegepersonal oder dem Patienten selbst durchgeführt werden müssen.

"**myoncare App**" meint die mobile myoncare Applikation zur Verwendung durch Patienten oder Mitarbeitern, die die von ONCARE angebotenen Dienste 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 Tools**" meint die myoncare App und das myoncare Portal gemeinsam.

"**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 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 jeden Gesundheitsdienstleister, jedes Unternehmen oder jeden Datendienstleister, der das webbasierte myoncare Portal nutzt.

"**Datenschutzerklärung**" meint diese Erklärung, die Ihnen als Patient und Nutzer der myoncare App gegenüber abgegeben wird und die beschreibt, wie wir Ihre personenbezogenen Informationen erfassen, nutzen und aufbewahren und die Sie über Ihre umfassenden Rechte informiert.

"**Nutzungsbedingungen**" bezeichnet die Nutzungsbedingungen für die Nutzung der myoncare App.

2. VERARBEITUNG VON (BEHANDLUNGS-)DATEN

Die Oncare GmbH, ein beim Amtsgericht München unter der Registernummer 219909 eingetragenes Unternehmen mit Sitz in der Balanstraße 71a, 81541 München, Deutschland, bietet die mobile Anwendung **myoncare App** an und betreibt diese als Zugang zu den **myoncare Services**. Diese **Datenschutzerklärung** gilt für alle personenbezogenen Daten, die von ONCARE im Zusammenhang mit der Nutzung der **myoncare App** verarbeitet werden.

3. WAS SIND PERSONENBEZOGENE DATEN

"**personenbezogene Daten**" bezeichnet alle Informationen, die es ermöglichen, eine natürliche Person zu identifizieren. Insbesondere beinhaltet dies Ihren Namen, Ihren 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 "**pseudonymisiert**" 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.

4. myoncare PWA

Eine Progressive Web App (PWA) ist eine Website, die aussieht und die Funktionalität einer mobilen App hat. PWAs sind so aufgebaut, dass sie die Vorteile der nativen Funktionen von Mobilgeräten nutzen, ohne dass der Nutzer einen App-Store benötigt. 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.

5. 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 unserer **myoncare App**, bei der Kontaktaufnahme zu Problemen mit der App oder bei sonstigen Interaktionen mit uns zum Zweck der Nutzung der App zur Verfügung stellen**.**

Daten zur Behandlung: Sie oder Ihr Gesundheitsdienstleister stellen uns Ihre personenbezogenen Daten wie Name, Alter, Größe, Gewicht, Indikation, Krankheitssymptome und andere Informationen im Zusammenhang mit Ihrer Behandlung (z. B. in einem Pflegeplan) zur Verfügung. Zu den Informationen im Zusammenhang mit Ihrer Behandlung gehören insbesondere: Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien, die von Ihrem **Leistungserbringer,** bereitgestellt wurden, geplante und erledigte Aufgaben.

Kommerzielle Store-Daten: Kommerzielle Store-Daten: Personenbezogene Daten, die im Zusammenhang mit der Nutzung des myoncare 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.

Verwendung anonymisierter Daten zu kommerziellen Zwecken: Zusätzlich kann ONCARE bestimmte Gesundheits- und Nutzungsdaten nach vollständiger Anonymisierung auch für kommerzielle Zwecke verwenden – etwa zur Weiterentwicklung der Plattform, zur Analyse von Versorgungsprozessen oder zur Entwicklung neuer digitaler Gesundheitsdienste. Die Anonymisierung erfolgt so, dass ein Rückschluss auf Ihre Person nicht mehr möglich ist. Diese Daten unterliegen daher nicht mehr der DSGVO.

Aktivitätsdaten: Personenbezogene Daten, welche von uns verarbeitet werden, falls Sie die **myoncare App** mit einer Gesundheitsapplikation verbinden (z.B. GoogleFit, AppleHealth, Withings). Ihre Aktivitätsdaten werden an Ihre verbundenen **Leistungserbringer** als **Portalnutzer** transferiert.

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.

Daten von Geräteherstellern, Inverkehrbringern medizinischer Geräte oder Laboren:

Zusätzlich können im Rahmen integrierter Versorgungsprozesse personenbezogene Daten durch angebundene medizinische Gerätehersteller, Inverkehrbringer medizinischer Geräte 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 zur Erfüllung der gesetzlichen Sicherheits- oder Vigilanzzwecke von Medizinprodukte- oder Pharmaunternehmen verarbeitet werden.

Kostenerstattungsdaten: Personenbezogene Daten, die für den Kostenerstattungsprozess zwischen Ihrem Leistungserbringer und Ihrer Krankenkasse erforderlich sind.

Daten zum betrieblichen Gesundheitsmanagement: Persönliche oder aggregierte Daten, die in konkreten Projekten und Fragebögen auf Anfrage Ihrer **Firma** (entweder direkt oder durch einen von Ihrem Unternehmen beauftragten Datendienstleister) erhoben werden. Die Daten können sich auf bestimmte Gesundheitsinformationen, Ihre Meinung über Ihr persönliches Wohlbefinden, Ihre Meinung als Mitarbeiter zu einer bestimmten internen oder externen Situation oder Daten über Pflege oder Gesundheit im Allgemeinen beziehen.

6. BLOCKCHAIN-TECHNOLOGIE

Die **Blockchain Technologie** ("**Blockchain**") (Europäisches Patent Nr. 4 002 787) ist ein optionaler Dienst, der nicht verpflichtend buchbar ist. Es ist Ihr **Leistungserbringer**, der sich für die Verwendung der Blockchain-Lösung entscheidet. 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.

Im Allgemeinen besteht die **Blockchain** aus digitalen Daten in einer Kette von Paketen, die als "Blöcke" bezeichnet 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. 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. In diesem Fall kann der Block nicht mehr mit den anderen synchronisiert werden. Dieser technische Prozess verhindert, dass Unbefugte die Inhalte der **Blockchain** Kette manipulieren können. Wenn alle Nodes (Netzwerkknoten) versuchen, ihre Kopien zu synchronisieren, wird erkannt, dass eine Kopie geändert wurde, und das Netzwerk betrachtet diesen Node als fehlerhaft.

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 "nicht autorisiert" sind, sind private **Blockchains** "autorisiert", da eine Autorisierung erforderlich ist, um Benutzer zu werden. Im Gegensatz zu öffentlichen **Blockchains**, die für jedermann öffentlich zugänglich sind, ist der Zugang zu privaten **Blockchains** abhängig von der Berechtigung, um Benutzer zu werden. Diese Struktur ermöglicht es, die Sicherheit und Unveränderlichkeit der Blockchain-Technologie zu nutzen und gleichzeitig datenschutzkonform zu sein und 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:

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

Die in der **Blockchain** gespeicherten Datei sind pseudo-anonymisiert.

Unsere **Blockchain** soll den Datenschutz gewährleisten, und zwar in Bezug auf die Integrität der Daten, das Patientenprofil, die Assets und die zugewiesenen **Caretask** und Medikationen. Um mit der **Blockchain** zu kommunizieren, muss der Benutzer eine Reihe von öffentlich-privaten Schlüsseln registrieren. Um mit der **Blockchain** zu kommunizieren, benötigt der Nutzer mehrere public-private Keys; der Registrierungsprozess erzeugt Zertifikate, die in einer separaten Datenbank des **Leistungserbringers** und auf dem Handy des Patienten gespeichert werden. Eine Sicherungskopie des Patienten Keys wird verschlüsselt und in der Datenbank des **Leistungserbringers** gespeichert, auf die nur der Patient seinerseits zugreifen kann.

Bei der Überprüfung der Einwilligung zum Datenschutz überprüft das System, im Falle, dass der **Leistungserbringer** mit dem Patienten kommunizieren will, ob der Patient seine Zustimmung zu den Datenschutzrichtlinien des **Leistungserbringers** erteilt hat. Die **Blockchain** dient daher, die Integrität und Verantwortlichkeit des Datensatzes zu gewährleisten, um sicherzugehen, dass der Patient die Datenschutzrichtlinie akzeptiert hat.

Wenn ein **Leistungserbringer** eine neue Version einer Datenschutzerklärung hochlädt, wird der Hash der Datei in der **Blockchain** gespeichert und nachdem der Patient seine Einwilligung erteilt hat, wird diese Interaktion in der **Blockchain** gespeichert. Bei jeder Kommunikation mit dem Patienten

antwortet die **Blockchain** durch den Vergleich des Hashs mit einer Flag (Markierung), die Auskunft darüber gibt, ob die Einwilligung des Patienten für die aktuelle Datenschutzrichtlinie noch gültig ist.

Auch bei der Patientensynchronisierung wird die Integrität des Patientenprofils durch die **Blockchain** gewährleistet. Der **Leistungserbringer** erkennt sofort, wenn das Patientenprofil mit dem Profil auf dem Handy nicht synchronisiert bzw. übereinstimmt, indem der Hash des Patientenprofils in der **Blockchain** verglichen wird. 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:
Die Patienten können sich mit der gleichen Blockchain-Instanz verbinden, und zwar mit Hilfe des Phone Manager Tools, welches ebenfalls von ONCARE gehostet wird. Dieser Service wird ebenfalls von ONCARE gehostet.

Rechtsgrundlage für die Datenverarbeitung: Die Datenverarbeitung durch ONCARE für den **Leistungserbringer** erfolgt auf der Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

7. VERARBEITUNG VON OPERATIVEN DATEN

Anwendbar für alle App-Nutzer

Sie können uns bestimmte personenbezogene Daten zur Verfügung stellen, wenn Sie sich mit uns in Verbindung setzen, um die Funktionen und die Nutzung der **myoncare App** zu verstehen, im Falle einer Serviceanforderung Ihrerseits oder im Falle von unsererseits initiierten (telefonischen) Unterstützungsangebot.

Service-Mitarbeiter
Im Auftrag des Datenverantwortlichen (bspw. Leistungserbringers) bieten wir Ihnen an, Sie beim Ausfüllen von Fragebögen telefonisch zu unterstützen (Outbound Calls), um Ihre digitale Patientenbegleitung zu optimieren. Sollten Sie dieses Angebot nicht nutzen wollen, steht es Ihnen frei, dieses nicht anzunehmen und der telefonischen Unterstützung zu widersprechen.

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

- Die personenbezogenen Daten, die Sie über unsere App Ihrem **Leistungserbringer** zur Verfügung gestellt haben (z. B. Name, Geburtsdatum, Profilbild, Kontaktdaten).

- Die Gesundheitsdaten, die Sie Ihrem **Gesundheitsdienstleister,** dem **Datendienstleister** oder dem **Arbeitgeber** über unsere **myoncare App** zur Verfügung gestellt haben (z. B. Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien von medizinischem Fachpersonal, geplante und erledigte Aufgaben).

Autorisierte ONCARE-Mitarbeiter, die zum Zweck der Bearbeitung einer Serviceanfrage oder eines Outbound Calls auf die Datenbank Ihres **Leistungserbringers**, **Datendienstleister** oder **Arbeitgeber** zugreifen können, sind vertraglich verpflichtet, alle personenbezogenen Daten streng vertraulich zu behandeln.

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

1. **Push-Benachrichtigungen**:
   - Wir senden Ihnen Push-Benachrichtigungen über unsere **myoncare-PWA** (Progressive WebApp) 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.
   - Dies stellt sicher, dass Sie keine wichtigen Benachrichtigungen verpassen und Ihre Betreuung reibungslos verläuft.

Warum wir dies tun:
- Unser Ziel ist es, Sie über Ihre Aufgaben und wichtige Updates auf dem Laufenden zu halten, um Ihre Gesundheit bestmöglich zu unterstützen.
- E-Mails sind ein zuverlässiger Weg, um sicherzustellen, dass wichtige Informationen Sie erreichen, auch wenn Push-Benachrichtigungen deaktiviert sind.

Ihre Handlungsmöglichkeiten:
- 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 operativen Daten fungiert ONCARE als Datenverantwortlicher, der für die rechtmäßige Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist.

Arten von Daten: Ihr Name, Ihre E-Mail-Adresse, Ihre Telefonnummer, Ihr Geburtsdatum, das Datum der Registrierung, die von der App generierten Pseudoschlüssel; Geräte-Token zur Identifizierung Ihres Geräts, Ihre Pseudo-Identifikationsnummer, Ihre IP-Adresse, Typ und Version des von Ihrem Gerät verwendeten Betriebssystems.

Wenn die **myoncare App** heruntergeladen wird, werden die notwendigen Informationen an den App-Store-Anbieter übermittelt. Wir haben keinen Einfluss auf diese Datenerhebung und sind dafür auch nicht verantwortlich. Wir verarbeiten die uns vom Anbieter des App-Stores im Rahmen unseres Vertragsverhältnisses zur Verfügung gestellten personenbezogenen Daten zum Zwecke der Weiterentwicklung unserer **myoncare Apps** und Services.

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 operativen Daten, um die Funktionalitäten der **myoncare App** 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, Hilfestellung beim Ausfüllen der Fragebögen, usw.).

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 App** abschließen, gerechtfertigt.

8. 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/

9. VERARBEITUNG VON (BEHANDLUNGS-)DATEN

Anwendbar für App-Nutzer, die die App mit ihrem Leistungserbringer nutzen.

Während der Nutzung der **myoncare-App** kann Ihr **Leistungserbringer** Ihre persönlichen Daten in das **myoncare-Portal** eingeben, um die **myoncare-Dienste** zu starten (z. B. Sie als Patient anlegen, Bereitstellung einer individuellen Aufgabe, Erinnerung zur Medikamenteneinnahme usw.). Zusätzlich können Sie und Ihr **Leistungserbringer** Dokumente und Dateien in die **myoncare-App** und das **myoncare-Portal** hochladen und miteinander teilen. Ihr **Leistungserbringer** kann eine **Datenschutzrichtlinie** zu Ihrer Information hochladen und weitere Zustimmungserfordernisse für Sie als Patient festlegen, für die Ihre Zustimmung erforderlich ist. Die Dateien werden in einer Cloud-Datenbank in Deutschland gespeichert. Ihr **Leistungserbringer** kann die Freigabe solcher Dateien mit anderen **Portalnutzern** innerhalb seiner Einrichtung oder anderen **Leistungserbringern** außerhalb seiner Einrichtung (Konsiliarärzte) für medizinische Zwecke ermöglichen. Andere Portalbenutzer haben ohne diese Freigabe keinen Zugriff auf diese Dateien. Ferner kann Ihr **Leistungserbringer** uns beauftragen, Sie telefonisch beim Ausfüllen von Fragebögen zu unterstützen (Outbound Calls). Dies erfolgt nur nach Anweisung Ihres Leistungserbringers und wird ausschließlich von autorisierten ONCARE Mitarbeitern durchgeführt.

Wir werden Ihre Daten in Übereinstimmung mit den in dieser **Datenschutzrichtlinie** festgelegten Bestimmungen verwenden und verarbeiten, vorausgesetzt Sie erteilen uns Ihre Zustimmung, soweit erforderlich.

Wir verarbeiten diese personenbezogenen Daten, einschließlich Ihrer Gesundheitsdaten, im Rahmen einer Vereinbarung mit und in Übereinstimmung mit den Anweisungen Ihres **Leistungserbringers**. Für diese Verarbeitungszwecke ist der **Leistungserbringer** im Sinne der geltenden Datenschutzgesetze als Datenverantwortlicher für die Verarbeitung Ihrer personenbezogenen Daten und Gesundheitsdaten verantwortlich, und ONCARE ist der Datenverarbeiter dieser personenbezogenen (Gesundheits-) Daten. Das bedeutet, dass ONCARE personenbezogene Daten nur nach den Weisungen des **Leistungserbringers** verarbeitet. Wenn Sie Fragen oder Bedenken bezüglich der Verarbeitung Ihrer personenbezogenen Daten oder Gesundheitsdaten haben, sollten Sie sich in erster Linie an Ihren **Leistungserbringer** wenden.

Arten von Daten: Name, Geburtsdatum, Profilinformationen, Kontaktdaten und auch Gesundheitsdaten, wie z.B. Symptome, Fotos, Informationen über eingenommene Medikamente, Fragebogenantworten einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien von medizinischem Fachpersonal, geplante und erledigte Aufgaben.

Zwecke der Datenverarbeitung: Wir verarbeiten Ihre Behandlungsdaten, um unseren **myoncare-Dienst** für Ihren **Leistungserbringer** und für Sie bereitzustellen. Ihre Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden von Ihrem **Leistungserbringer** zur Beratung und Unterstützung für Sie verwendet. Wir verarbeiten diese personenbezogenen Daten im Rahmen einer Vereinbarung mit und in Übereinstimmung mit den Anweisungen Ihres **Leistungserbringers**. Die Übertragung dieser Behandlungsdaten erfolgt pseudonymisiert und verschlüsselt. Zur Ausübung Ihrer Betroffenenrechte wenden Sie sich bitte an Ihre **Leistungserbringer**.

Rechtfertigung der Verarbeitung von Behandlungsdaten: Ihre personenbezogenen (Behandlungs-) Daten werden von Ihrem **Leistungserbringer** gemäß den Bestimmungen der **DSGVO** und aller anderen geltenden Datenschutzvorschriften verarbeitet. Rechtsgrundlagen für die Datenverarbeitung ergeben sich insbesondere aus Art. 9 Abs. 2 lit. h DSGVO für Gesundheitsdaten als besonders schützenswerte Daten sowie Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a und 9 Abs. 2 lit. a DSGVO. Die Verarbeitung von Daten durch ONCARE für Ihre **Leistungserbringer** erfolgt darüber hinaus auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).
Ihr **Leistungserbringer** ist als Datenbeauftragter für die Einholung Ihrer Einwilligung verantwortlich. Auch wenn Sie die **myoncare App** ohne eine solche Einwilligung nutzen können, funktionieren die meisten Funktionen nicht mehr (z. B. die Weitergabe von Daten an Ihren Gesundheitsdienstleister). Die Verweigerung oder der Widerruf der Einwilligung in die Verarbeitung von Behandlungsdaten führt daher zu einer starken Einschränkung der Funktionalität der App-Dienste und Ihre **Leistungserbringer** können Sie nicht mehr über die **myoncare App** unterstützen.

10. VERARBEITUNG VON AKTIVITÄTSDATEN

Nur anwendbar, wenn Sie der Aktivitätsdatenübertragung über myoncare Tools zustimmen und diese aktivieren.

myoncare Tools bieten Ihnen die Möglichkeit, die **myoncare App** mit bestimmten Gesundheits-Apps (z. B. AppleHealth, GoogleFit, Withings), zu verbinden, die Sie nutzen (**"Health App"**). Um die Verarbeitung von Aktivitätsdaten zu ermöglichen, holen wir vorab Ihre Einwilligung in die Verarbeitung ein. Wenn die Verbindung nach Ihrer Einwilligung hergestellt wird, werden die von der **Health-App** gesammelten Aktivitätsdaten Ihren **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen. Bitte beachten Sie, dass Aktivitätsdaten nicht von **myoncare Tools** validiert werden und von Ihrem **Leistungserbringer** nicht für diagnostische Zwecke als Basis der medizinischen Entscheidungsfindung genutzt werden sollen. Bitte beachten Sie auch, dass Ihre **Leistungserbringer** nicht verpflichtet sind, Ihre Aktivitätsdaten zu überprüfen und Ihnen keine Rückmeldung zu Ihren Aktivitätsdaten geben müssen.
Aktivitätsdaten werden jedes Mal, wenn die **myoncare-App** aufgerufen wird, mit Ihren angeschlossenen **Leistungserbringern** geteilt. Sie können Ihre Einwilligung zur Weitergabe von Aktivitätsdaten jederzeit in den Einstellungen der **myoncare App** widerrufen. Bitte beachten Sie, dass Ihre Aktivitätsdaten ab diesem Zeitpunkt nicht mehr weitergegeben werden. Aktivitätsdaten, die bereits geteilt wurden, werden nicht aus dem **myoncare-Portal** Ihrer angeschlossenen **Leistungserbringer** gelöscht.

Die Verarbeitung von Aktivitätsdaten liegt in Ihrer eigenen Datenverantwortung.

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

Zweck der Verarbeitung von Aktivitätsdaten: Ihre Aktivitätsdaten werden Ihren verbundenen **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen.

Rechtfertigung der Verarbeitung: Die Verarbeitung von Aktivitätsdaten unterliegt Ihrer eigenen Verantwortung.

11. VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

Anwendbar für App-Nutzer, deren Leistungserbringer die Medizinproduktvariante der myoncare Tools verwendet.

Die **myoncare App** ist als Medizinprodukt gemäß den europäischen Medizinprodukteverordnungen klassifiziert und vermarktet. Als Hersteller der App müssen wir bestimmte gesetzliche Verpflichtungen einhalten (z.B. Überwachung der Funktionalität der App, Auswertung von Vorfallmeldungen, die mit der Nutzung der App in Verbindung stehen könnten, Tracking von Nutzern etc.). Zusätzlich ermöglicht die **myoncare-App** Ihnen und Ihrem **Leistungserbringer**, zu kommunizieren und persönliche Daten über bestimmte medizinische Geräte oder Medikamente, die in Ihrer Behandlung verwendet werden, zu erfassen. Die Hersteller solcher Medizinprodukte oder Arzneimittel haben auch gesetzliche Verpflichtungen hinsichtlich der Marktüberwachung (z.B. Sammlung und Bewertung von Nebenwirkungsmeldungen).

ONCARE ist der Datenverantwortliche für die Verarbeitung von Produktsicherheitsdaten.

Arten von Daten: Fallberichte, personenbezogene Daten, die in einem Vorfallbericht bereitgestellt wurden, und Ergebnisse der Auswertung.

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. Zusätzlich speichern und übertragen wir personenbezogene Daten im Zusammenhang mit medizinischen Geräten und/oder Medikamenten, wenn wir Mitteilungen von Ihrem **Leistungserbringer**, von Ihnen als Patient 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.

Rechtfertigung der Verarbeitung von Produktsicherheitsdaten: Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung rechtlicher Verpflichtungen als Medizinprodukte- oder Arzneimittelhersteller 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.

Ergänzung zum Haftungsauschluss 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 VON GESUNDHEITS- bzw. BEHANDUNGSDATEN

Anwendbar für App-Nutzer, die die App mit ihrem Leistungserbringer für Kostenerstattungszwecke verwenden.

Die **myoncare-App** unterstützt Ihren **Leistungserbringer** bei der Einleitung standardmäßiger Verfahren zur Kostenerstattung für die Gesundheitsleistungen, die Ihnen über die **myoncare-App** bereitgestellt werden. Um den Erstattungsprozess zu ermöglichen, unterstützt die **myoncare-App** die Erfassung Ihrer personenbezogenen (Gesundheits-) Daten durch Ihren **Leistungserbringer** zur Übermittlung dieser Daten an Ihre zahlende Stelle (entweder die Kassenärztliche Vereinigung und/oder Ihre Krankenversicherung). Diese Datenverarbeitung ist nur eine initiale Datenübermittlung für den **Leistungserbringer**, um eine Kostenerstattung von Ihrer Krankenversicherung zu erhalten. Die Art und Menge der verarbeiteten personenbezogenen Daten unterscheidet sich nicht von anderen Erstattungsroutinen des **Leistungserbringers**. Ihr Leistungserbringer ist der Datenbeauftragte für Erstattungsdaten. ONCARE agiert als Datenverarbeiter auf der Grundlage der Datenverarbeitungsvereinbarung mit Ihrem **Leistungserbringer**.

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

Verarbeitung von Erstattungsdaten: Ihr **Leistungserbringer** übermittelt die für die Erstattung erforderlichen Behandlungsdaten an den Kostenträger (entweder seine gesetzliche Krankenversicherungseinrichtung und/oder Ihre Krankenversicherung), und der Kostenträger verarbeitet die Erstattungsdaten, um die Erstattung an Ihren **Leistungserbringer** zu leisten.

Rechtfertigung der Verarbeitung von Erstattungsdaten: Die Erstattungsdaten werden auf Grundlage der §§ 295, 301 SGB V, Art. 9 Abs. 2 lit. b DSGVO verarbeitet. Die Datenverarbeitung durch ONCARE für Ihren **Leistungserbringer** erfolgt ebenfalls auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

13. VERARBEITUNG DURCH GERÄTEHERSTELLER, INVERKEHRBRINGER MEDIZINISCHER GERÄTE 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, Inverkehrbringer solcher 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.

14. 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.

15. VERARBEITUNG VON DATEN DES BETRIEBLICHEN GESUNDHEITSMANAGEMENTS

Anwendbar für Nutzer der App, die die App mit dem betrieblichen Gesundheitsmanagement der Firma verwenden.

Während der Nutzung der **myoncare-App** im **betrieblichen Gesundheitsmanagement** des Unternehmens werden bestimmte personenbezogene (Gesundheits-)Daten in aggregierter Form als Daten für das betriebliche Gesundheitsmanagement an das **Unternehmen** und die von dem **Unternehmen** beauftragten **Datenanbieter** (z. B. Datenanalysten oder Forschungsunternehmen) weitergegeben. Weder das **Unternehmen** noch ein **Datendienstleister** können solche Daten Ihrer Identität zuordnen. ONCARE empfiehlt, während der Nutzung der **myoncare-Dienste** im Rahmen des betrieblichen Gesundheitsmanagements keine persönlichen Daten zu teilen.

Das bedeutet, dass ONCARE und alle **Datenanbieter** die Daten für das betriebliche Gesundheitsmanagement nur gemäß den Anweisungen des **Unternehmens** verarbeiten werden. Wir verarbeiten solche Daten für das betriebliche Gesundheitsmanagement, einschließlich Ihrer Gesundheitsdaten, auf der Grundlage einer Vereinbarung mit Ihrem **Unternehmen** und/oder einem **Datenanbieter** und gemäß deren Anweisungen. Für die Zwecke dieser Vereinbarung ist das **Unternehmen** oder der **Datenanbieter** der Datenverantwortliche für die Verarbeitung Ihrer Daten zu Zwecken des betrieblichen Gesundheitsmanagements, und ONCARE sowie alle vom **Unternehmen** beauftragten **Datenanbieter** sind die Datenverarbeiter dieser Daten. Wenn Sie Fragen oder Bedenken hinsichtlich der Verarbeitung Ihrer Daten für das betriebliche Gesundheitsmanagement haben, sollten Sie sich in erster Linie an das **Unternehmen** wenden**.**

Zwecke der Datenverarbeitung im betrieblichen Gesundheitsmanagement: Wir verarbeiten Ihre Daten für das betriebliche Gesundheitsmanagement, um Ihnen und dem **Unternehmen** unsere **myoncare-Dienste** anbieten zu können. Ihre Daten zum betrieblichen Gesundheitsmanagement, die Sie in unsere **myoncare-App** eingeben, werden vom **Unternehmen** (entweder direkt oder über einen **Datenanbieter**) im Rahmen des betrieblichen Gesundheitsmanagements verwendet. Wir verarbeiten diese Daten für das betriebliche Gesundheitsmanagement im Rahmen einer Vereinbarung mit und gemäß den Anweisungen des **Unternehmens** und/oder eines **Datenanbieters** für dessen betriebliches Gesundheitsmanagement. Die Übertragung dieser Daten für das betriebliche Gesundheitsmanagement erfolgt pseudonymisiert und verschlüsselt. Zur Ausübung Ihrer Betroffenenrechte wenden Sie sich bitte an das **Unternehmen**.

Rechtfertigung der Verarbeitung von Daten zum betrieblichen Gesundheitsmanagement: Ihre Daten zum betrieblichen Gesundheitsmanagement werden vom **Unternehmen** gemäß den Bestimmungen der **DSGVO** und aller anderen geltenden Datenschutzvorschriften

verarbeitet. Rechtsgrundlage für die Datenverarbeitung ist insbesondere Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. eine DSGVO oder eine andere für das **Unternehmen** geltende rechtliche Grundlage. Die Verarbeitung von Daten durch ONCARE für das **Unternehmen** (entweder direkt oder über einen von Ihrem Unternehmen beauftragten **Dienstleister**) basiert ebenfalls auf Art. 28 DSGVO (Auftragsverarbeitungsvertrag).
Das **Unternehmen** ist als Datenverantwortlicher dafür verantwortlich, Ihre Einwilligung einzuholen, wenn dies durch Datenschutzvorschriften erforderlich ist, und die Daten für Zwecke des betrieblichen Gesundheitsmanagements gemäß den geltenden Datenschutzgesetzen zu verarbeiten.

16. WELCHE TECHNOLOGIE WIRD VON DER MYONCARE APP VERWENDET?

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 von Push-Benachrichtigungen durch E-Mails für **PWA** (Progressive Web App) in den folgenden Fällen:
  - → wenn ein Careplan in einer Stunde 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** eine **Caretask** zugewiesen hat.

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

SendGrid (englisch) (Datenschutzerklärung):
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 "permanenter 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:

- Benutzerrolle;
- Geolokalisierung des Benutzers;
- Benutzer-Betriebssystem;
- Zeit, zu der der Nutzer Inhalte verwendet hat;
- -IP-Adresse;
- Websites, die über das Web / besucht werden **PWA** (Weitere Informationen finden Sie im Abschnitt über PWA in dieser Datenschutzrichtlinie);
- Schaltflächen, die der Benutzer im **myoncare-Portal**, der **myoncare-App** und 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 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.

17. 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 zur und von der App erfolgt verschlüsselt. Wir verwenden TLS und SSL als Verschlüsselungsprotokolle für eine sichere Datenübertragung. Auch der Datenaustausch ist durchgehend verschlüsselt und erfolgt mit Pseudoschlüsseln.

18. 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).

Jede Übertragung personenbezogener Daten wird während der Übertragung verschlüsselt.

19. 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 die myoncare-App Sie im Rahmen des Einwilligungsverfahrens ausdrücklich darüber informieren.
Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darf nur erfolgen, wenn dies gesetzlich vorgeschrieben 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 der myoncare App verwaltet werden.
Ein Widerruf Ihrer Einwilligung wirkt ausschließlich für die Zukunft. Die bis zum Zeitpunkt des Widerrufs erfolgte Verarbeitung bleibt rechtmäßig (Art. 7 Abs. 3 DSGVO).

20. 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 erforderlich sind. Ihre persönlichen Daten und Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden entweder direkt oder über einen **Datenanbieter** Ihrem **Leistungserbringer** und/oder Ihrem **Unternehmen** zur Verfügung gestellt (abhängig von der Art der Nutzung der **myoncare-Tools**).

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. Diese Dienstleister sind Google (Google Firebase), Anbieter von Cloud-Speichern und Support-Dienstleistern.

Google Firebase ist eine "NoSQL-Datenbank", die die Synchronisation 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 der **myoncare-App** zusammen mit dem entsprechenden **Medikationsplan** 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 zwischen Ihnen und Ihrem **Dienstleister** oder **Unternehmen** (entweder direkt oder an einen **Datenanbieter**) verschlüsselt und Pseudokeys anstelle persönlicher Kennungen wie Name oder E-Mail-Adresse zur Nachverfolgung dieser Übertragungen verwendet werden. Die Re-Identifizierung erfolgt, sobald die personenbezogenen Daten das Konto Ihres **Leistungserbringers** oder Unternehmens im **myoncare-Portal** oder Ihr Konto in der **myoncare-App** erreicht haben, nachdem sie durch spezielle Tokens verifiziert wurden.

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 Ihre persönlichen Daten gespeichert werden. Es hostet auch die Video- und Dateiverwaltungsdienste von myoncare, die verschlüsselte Videokonferenzen zwischen Ihnen und Ihrem **Leistungserbringer** sowie den Austausch von Dateien ermöglichen. Der Zugriff auf Ihre persönlichen Daten durch Sie und Ihren **Leistungserbringer** wird durch das Senden spezifischer Tokens gewährleistet. Diese personenbezogenen Daten werden während der Übertragung und im Ruhezustand verschlüsselt und für ONCARE und seine Dienstleister 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 werden sie weiterhin von speziell zugelassenen ONCARE-Mitarbeitern verarbeitet, wie unter "VERARBEITUNG VON OPERATIVEN DATEN" beschrieben.

Über unsere Support-Dienstleister verwenden wir das RepairCode-Tool, 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 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 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

21. 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.
Die persönlichen Daten, die von dieser **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 der **myoncare-App** und des **myoncare-Portals** erfolgt über Google Firebase. Der Google Firebase-Server wird in der Europäischen Union gehostet. Wie in den Nutzungsbedingungen von Google Firebase beschrieben, sind jedoch kurzfristige Datenübermittlungen in Länder möglich, in denen Google oder seine Dienstanbieter ansässig sind; 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. Unrechtmäßiger Zugriff auf Ihre Daten wird mit Ende-zu-Ende-Verschlüsselung und sicheren Zugriffstoken verhindert. Unsere Server werden in Deutschland und für US-Kunden in den USA 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.

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.

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. Darüber hinaus wurden ergänzende technische Schutzmaßnahmen implementiert, wie die Ende-zu-Ende-Verschlüsselung sowie die strikte Zugriffsbeschränkung durch rollenbasierte Token. Dies dient der weiteren Absicherung der Datenübermittlung im Sinne des „Schrems II"-Urteils des EuGH.

Zur Verarbeitung von Aktivitätsdaten werden auf dem mobilen Gerät des **App-Benutzers** Schnittstellen zu Google Cloud-Diensten (im Fall von GoogleFit) oder zu AppleHealth oder Withings verwendet. **myoncare-Tools** verwenden diese Schnittstellen, die von Google, Apple und Withings bereitgestellt werden, um Aktivitätsdaten von 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.

22. 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, aber nicht ausschließlich, für handels- oder steuerrechtliche Aufbewahrungspflichten (z.B. Handelsgesetzbuch, Steuergesetz, etc.). Darüber hinaus muss Ihr **Leistungserbringer** auch die Aufbewahrung Ihrer medizinischen Unterlagen sicherstellen (je nach Art der Dokumente zwischen 1 und 30 Jahren).

Bitte beachten Sie, dass ONCARE auch Aufbewahrungspflichten unterliegt, die mit Ihrem **Leistungserbringer** aufgrund der gesetzlichen Bestimmungen vertraglich vereinbart werden. Darüber hinaus, und nur wenn Ihr **Leistungserbringer** die Medizinproduktvariante der **myoncare-Tools** verwendet, gelten aufgrund der Einstufung der **myoncare-App** als Medizinprodukt bestimmte Aufbewahrungsfristen, die sich aus dem Medizinproduktgesetz 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.

23. VERPLICHTUNG ZUR ANGABE 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. Das Gleiche gilt für die Nutzung unserer myoncare-App und die verschiedenen Funktionen, die sie bietet.

Die Details haben wir für Sie unter den oben genannten Punkten zusammengefasst. 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.

24. ZUGRIFFSRECHTE

Für alle Geräte, unabhängig vom verwendeten Betriebssystem, ist es notwendig, der App bestimmte Berechtigungen zu erteilen, die wir als "grundlegende Zugriffsrechte" bezeichnen. Abhängig vom Betriebssystem des Geräts, das Sie verwenden, verfügt es möglicherweise über zusätzliche Funktionen, die zusätzliche Berechtigungen erfordern, damit die App funktioniert. Damit die **myoncare-App** auf Ihrem Gerät funktioniert, muss der App verschiedene Berechtigungen erteilt werden, um auf bestimmte Funktionen des Geräts zuzugreifen. Gegebenenfalls werden wir sie in der Reihenfolge des Betriebssystems (Android oder iOS) gemäß den "Rahmenbedingungen" auflisten.
Die grundlegenden Zugriffsrechte (Android und iOS) sind:

WLAN-Verbindungen abrufen
Erforderlich, um die Funktionalität des Dokumentendownloads in Verbindung mit Wi-Fi-Verbindungen sicherzustellen.

Netzwerk-Verbindung abrufen
Erforderlich, um die Funktionalität des Dokumentdownloads in Verbindung mit Netzwerkverbindungen sicherzustellen, bei denen es sich nicht um Wi-Fi-Verbindungen handelt.

Bildschirmsperre deaktivieren (Stand-by-Modus verhindern)
Erforderlich, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne durch eine Bildschirmsperre unterbrochen zu werden.

Zugang zu allen Netzwerken
Zum Herunterladen von Dokumenten ist der Zugang zu allen Netzwerken erforderlich.

Deaktivieren des Schlafmodus
Dies ist notwendig, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne dass die Wiedergabe durch das Auftreten des Ruhezustands unterbrochen wird.

Mobile Daten / Zugriff auf mobile Daten
Möchte der Nutzer Dokumente ausschließlich über WLAN herunterladen, kann er im Menü der App die entsprechende Einstellung vornehmen und die Nutzung mobiler Daten deaktivieren. Der Zugriff auf mobile Daten ist erforderlich, um die Funktionalität der Deaktivierung von Dokumentendownloads über mobile Daten sicherzustellen.

Zugriff auf die Kamera
Sowohl für das Scannen von QR-Codes als auch für Videokonsultationen ist ein Kamerazugang erforderlich

Zugriff auf das Mikrofon
Für Videosprechstunden ist ein Mikrofonzugang erforderlich

Zugriff auf Dateien und Fotos
Dies ist für den Austausch von Dateien zwischen Ihnen und Ihren verbundenen Portalbenutzern erforderlich.

Zugriff auf den Webbrowser
Dies ist erforderlich, um empfangene Dateien von Benutzern des verbundenen Portals anzuzeigen.

Wir verwenden Push-Benachrichtigungen, bei denen es sich um Nachrichten handelt, die als Service der **myoncare-App** über Dienste wie den Apple Push Notification Service oder den Google Cloud Messaging Service an Ihr mobiles Gerät gesendet werden. Diese Dienste sind Standardfunktionen von Mobilgeräten. Die Datenschutzrichtlinie des Dienstanbieters regelt den Zugriff, die Verwendung und die Offenlegung personenbezogener Daten infolge Ihrer Nutzung dieser Dienste.

25. AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL

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

26. 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:

Auskunftsrecht (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, die **myoncare-App** einschließlich Ihrer

UID (Unique Identification Number) von Ihrem Smartphone/Handy 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 uns auffordern, unrichtige personenbezogene Daten zu aktualisieren oder zu korrigieren oder unvollständige personenbezogene Daten zu 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.

Widerspruchsrecht 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. Ein Widerruf wirkt ausschließlich für die Zukunft. Die bis zum Zeitpunkt des Widerrufs erfolgte Verarbeitung bleibt rechtmäßig.

Um diese Rechte auszuüben, wenden Sie sich bitte zunächst an Ihren **Leistungserbringer** oder Ihr **Unternehmen** oder kontaktieren Sie uns unter: 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 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.

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

28. ALTERSBESCHRÄNKUNG DER ANWENDUNG

Ein Mindestalter von 18 Jahren ist erforderlich, um die **myoncare-App** zu nutzen.

29. ÄNDERUNGEN DER DATENSCHUTZERKLÄRUNG

Wir behalten uns ausdrücklich das Recht vor, diese **Datenschutzerklärung** in Zukunft nach unserem alleinigen 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 in einem angemessenen Zeitrahmen mitgeteilt, bevor sie in Kraft treten (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, Deutschland

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

Kontaktdaten des Datenschutzbeauftragten: privacy@myoncare.com

Für Transaktionen im myoncare Store – insbesondere im Zusammenhang mit Behandlungsplänen (Pathways) – liegt die wirtschaftliche und inhaltliche Verantwortung bei der myon.clinic GmbH, einer Tochtergesellschaft der Oncare GmbH. Die Oncare GmbH stellt in diesem Kontext ausschließlich die technische Plattform zur Verfügung.

Zuletzt aktualisiert im Juni 2025.

* * *

Es folgen die ergänzenden Datenschutzregelungen für Nutzer in den Vereinigten Staaten von Amerika:

HIPAA schützt personenbezogene Gesundheitsdaten (PHI) nur dann, wenn sie im Kontext des US-Gesundheitssystems durch eine HIPAA-pflichtige Stelle – also eine Covered Entity oder einen Business Associate – verarbeitet werden, unabhängig von Staatsbürgerschaft oder Wohnsitz der betroffenen Person.

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

Geltungsbereich:
Dieser Abschnitt ergänzt die Datenschutzerklärung für Nutzer mit Wohnsitz in den Vereinigten Staaten von Amerika (USA) oder für Fälle, in denen Gesundheitsdaten *(*Protected Health Information – PHI*)* gemäß dem Health Insurance Portability and Accountability Act (HIPAA) verarbeitet werden.

Er gilt in sämtlichen Bundesstaaten der USA, soweit ONCARE oder beauftragte Partner als *Business Associate* im Auftrag von *Covered Entities* (z. B. Ärzten oder Kliniken) Gesundheitsdaten im Rahmen von Behandlungsprozessen verarbeitet.

1. Rechtliche Grundlagen in den USA

Die Verarbeitung personenbezogener Gesundheitsdaten in den USA unterliegt dem **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** sowie nachfolgenden Ergänzungen, insbesondere:

- der **HIPAA Privacy Rule** (45 CFR Part 160 & Subparts A and E of Part 164)
- der **HIPAA Security Rule** (Subparts A and C of Part 164)
- der **HIPAA Breach Notification Rule** (Subpart D of Part 164)
- sowie ergänzend ggf. dem HITECH Act von 2009

Diese Regelungen gelten unabhängig davon, in welchem Bundesstaat der USA sich der Patient oder die verarbeitende Stelle befindet.

2. Rolle von ONCARE als Business Associate

Die ONCARE GmbH sowie verbundene Unternehmen in den USA handeln ausschließlich als sogenannte **Business Associates** im Sinne des HIPAA, wenn sie im Auftrag von Gesundheitsdienstleistern **(*Covered Entities*)** Leistungen im Zusammenhang mit der Verarbeitung von PHI erbringen. Ein Business Associate Agreement (BAA) gemäß 45 CFR §164.504(e) regelt die datenschutzrechtlichen Verpflichtungen gegenüber diesen Einrichtungen. ONCARE übernimmt in diesem Rahmen:

- Bereitstellung der myoncare-Plattform (Video, Kommunikation, Monitoring)
- technische Datenverarbeitung & Hosting
- Bereitstellung algorithmischer Unterstützungsfunktionen (z. B. Triage)

ONCARE erbringt **keine medizinischen Leistungen** und trifft **keine medizinischen Entscheidungen** im Sinne einer Diagnose, Therapie oder Verschreibung.

3. Art der verarbeiteten Daten (PHI)

Als PHI im Sinne des HIPAA gelten alle Informationen, die:

- sich auf den Gesundheitszustand oder die Behandlung eines identifizierbaren Patienten beziehen, und
- in Verbindung mit einer *Covered Entity* oder deren Business Associate verarbeitet werden.

Zu den durch ONCARE verarbeiteten PHI gehören insbesondere:

- anamnestische Angaben (Symptome, Risikofaktoren)
- Monitoringdaten (Vitalparameter, Wearable-Daten)
- Nutzerinteraktionen innerhalb strukturierter Fragebögen oder Triage-Tools
- Kommunikationsverläufe mit Gesundheitsdienstleistern

4. Patientenrechte gemäß HIPAA

Jeder betroffene Nutzer in den USA hat das Recht auf:

- **Auskunft** über die zu seiner Person gespeicherten PHI (45 CFR §164.524)
- **Berichtigung** fehlerhafter oder unvollständiger PHI (45 CFR §164.526)
- **Einschränkung** der Offenlegung oder Nutzung in bestimmten Fällen (45 CFR §164.522)
- **vertrauliche Kommunikation** auf Wunsch des Patienten

- **Widerspruch** gegen bestimmte Weitergaben (soweit gesetzlich zulässig)
- **Auskunft über Datenweitergaben** (Accounting of Disclosures, 45 CFR §164.528)
- **Beschwerde** bei der zuständigen Datenschutzbehörde des US-Gesundheitsministeriums (Office for Civil Rights)

ONCARE stellt technische Schnittstellen bereit, um diese Rechte auf Anfrage umzusetzen.

Um diese Rechte geltend zu machen, können Sie eine formlose Anfrage über die myoncare App stellen oder uns per E-Mail kontaktieren. Die Umsetzung erfolgt in der Regel innerhalb von 30 Tagen gemäß 45 CFR §164.524 ff. Sofern die Anfrage komplex ist, kann die Frist einmalig um weitere 30 Tage verlängert werden. ONCARE stellt hierfür digitale Exportformate und Zugriffsschnittstellen bereit.

5. Sicherheitsmaßnahmen gemäß Security Rule

ONCARE verpflichtet sich zur Einhaltung aller Anforderungen aus der HIPAA Security Rule, insbesondere:

Administrative Maßnahmen

- interne Datenschutz- und Zugriffskonzepte
- schriftliche Richtlinien zur Zugriffsregelung
- Risikoanalysen und regelmäßige Audits
- Mitarbeiterschulung mit HIPAA-Fokus

Darüber hinaus verpflichtet sich ONCARE zur regelmäßigen Durchführung eines strukturierten „Security Risk Assessments“ gemäß 45 CFR §164.308(a)(1)(ii)(A), um Sicherheitsrisiken zu identifizieren, zu bewerten und angemessene Maßnahmen zu ergreifen.

Technische Maßnahmen

- Verschlüsselung aller ruhenden und übermittelten PHI
- rollenbasierte Zugriffskontrolle
- Logging und Zugriffshistorie
- Zwei-Faktor-Authentifizierung für medizinisches Personal

Physische Maßnahmen

- sichere Serverstandorte mit Zugangskontrolle
- Notfallwiederherstellungskonzepte
- Zugriffsbeschränkungen für Hardware und Endgeräte

6. Datenschutz bei automatisierter Triage

Die myoncare-Plattform enthält eine strukturierte Triage-Funktion, die Patienteninformationen (z. B. Symptome) auf Basis festgelegter Kriterien auswertet und **eine technische Risikobewertung** erstellt.

Diese Funktion:

- **ersetzt keine medizinische Diagnose**,
- **entscheidet nicht selbstständig über Behandlung oder Intervention**,
- **informiert lediglich autorisierte Leistungserbringer** (Covered Entity) über potenziell relevante Informationen.

ONCARE trägt keine medizinische Verantwortung für Entscheidungen, die auf Grundlage dieser Informationen durch Ärzte oder Kliniken getroffen werden.

7. Offenlegung von PHI und weitere Verwendung

ONCARE gibt PHI ausschließlich weiter:

- an berechtigte Gesundheitsdienstleister im Rahmen der Versorgung,

- an Aufsichtsbehörden bei gesetzlicher Verpflichtung,
- bei Sicherheitsvorfällen im Rahmen der **Breach Notification Rule** (innerhalb von 60 Tagen ab Kenntnis gemäß 45 CFR §164.404),
- niemals zu Werbe-, Vertriebs- oder Drittnutzungszwecken ohne ausdrückliche, dokumentierte Zustimmung des Patienten.

Eine Weitergabe oder Nutzung von PHI für Forschungs-, Marketing- oder sonstige Drittzwecke erfolgt ausschließlich nach vorheriger dokumentierter „Authorization" gemäß 45 CFR §164.508. Ohne diese ausdrückliche Einwilligung findet keine solche Weitergabe statt.

Verwendung de-identifizierter Daten zu kommerziellen Zwecken
ONCARE kann Gesundheits- und Nutzungsdaten, die gemäß den Vorgaben der HIPAA-Datenschutzregelung (45 CFR §164.514) de-identifiziert wurden, zu internen Analysezwecken, zur Weiterentwicklung der Plattform, zur Entwicklung neuer Versorgungsmodelle sowie zu anderen kommerziellen Zwecken verwenden. Sobald die Daten de-identifiziert wurden, gelten sie nicht mehr als geschützte Gesundheitsdaten („Protected Health Information", PHI) und unterliegen nicht mehr den Vorgaben der HIPAA-Datenschutzregelung.

8. Kontakt zur Wahrnehmung von Rechten

Verantwortlich für HIPAA-bezogene Anliegen:
ONCARE GmbH
Balanstraße 71a
80339 München
Germany
E-Mail: privacy@myoncare.com

US-Bürger können sich bei Beschwerden auch direkt an das **U.S. Department of Health and Human Services – Office for Civil Rights (OCR)** wenden: https://www.hhs.gov/ocr/

9. Einbindung von Drittanbietern, Webshop-Daten und Haftungsausschluss

9.1 Einbindung technischer Drittanbieter (Gerätehersteller, Inverkehrbringer medizinischer Geräte und Labore)

Im Rahmen der Plattform myoncare und der Tochterfirma myon.clinic können bei Bedarf **Drittanbieter wie Gerätehersteller, Inverkehrbringer medizinischer Geräte oder medizinische Labore** an das System angebunden werden. Dies erfolgt ausschließlich zur Unterstützung der ärztlich verantworteten Versorgung und basiert auf den Anweisungen der jeweiligen *Covered Entities*.

Die angebundenen Drittanbieter verarbeiten personenbezogene Gesundheitsdaten (PHI) ausschließlich nach vertraglicher Vereinbarung und unter Beachtung der HIPAA-Vorgaben. Sie unterliegen ebenfalls den datenschutzrechtlichen Anforderungen gemäß 45 CFR §164.502(e) als *Subcontractors* eines Business Associates und werden durch entsprechende **Unterauftragsvereinbarungen (Sub-BAA)** verpflichtet.

9.2 Datenerhebung im Rahmen von Webshop-Angeboten

Bei Erwerb von digitalen Gesundheitsprogrammen, sog. **Pathways**, oder Affiliate-Produkten über den Webshop der Tochtergesellschaft **myon.clinic** können zur Abwicklung und Betreuung dieser Programme personenbezogene Daten einschließlich PHI verarbeitet werden. Dies betrifft insbesondere:

- Nutzungsdaten der Pathway-Funktionalität,
- angegebene Symptom- oder Diagnosedaten,
- ggf. eingelöste Gesundheitscodes oder Produktinformationen.

Die Erhebung erfolgt unter Beachtung der HIPAA-Privacy- und Security-Rules und ausschließlich zweckgebunden. Eine Weitergabe an Drittanbieter erfolgt nur auf Grundlage eines bestehenden Sub-BAA oder mit dokumentierter Einwilligung.

Jede Offenlegung von PHI (Protected Health Information) außerhalb der Vertragskette (z. B. für Forschung oder Marketing) bedarf einer dokumentierten **„Authorization"** nach 45 CFR §164.508.

9.3 Haftungsausschluss für medizinische Bewertung und Nebenwirkungen

Die ONCARE GmbH und ihre verbundenen Unternehmen übernehmen **weder eine medizinische Bewertung noch eine Verpflichtung zur Meldung von unerwünschten Arzneimittelwirkungen, Produktnebenwirkungen oder sonstigen gesundheitsbezogenen Risiken.**

Die rechtliche Verantwortung für:

- die Diagnose und Auswahl eines Pathways oder Produkts,
- die Bewertung von Risiken oder Kontraindikationen,
- sowie die gesetzlich vorgeschriebene **Meldung von Nebenwirkungen** oder Sicherheitsereignissen gegenüber Aufsichtsbehörden oder Herstellern

liegt ausschließlich beim behandelnden Arzt oder der anbietenden **Covered Entity** bzw. beim verantwortlichen Geräte- oder Arzneimittelhersteller.

Die Plattform stellt **lediglich die technische Infrastruktur** zur Verfügung und übernimmt keinerlei medizinische oder regulatorische Verantwortung für die Inhalte, Ergebnisse oder Folgewirkungen einer Anwendung durch Patienten oder Leistungserbringer.

10. Verhältnis zu bundesstaatlichem Recht (Preemption Rule & State Law Compliance)

Der Health Insurance Portability and Accountability Act (HIPAA) stellt ein **bundesrechtliches Mindestniveau** des Datenschutzes bereit, das in allen US-Bundesstaaten gilt. Gleichzeitig erlaubt 45 CFR §160.203 eine sogenannte **Preemption**, d. h. strengere Regelungen einzelner Bundesstaaten können den HIPAA in bestimmten Punkten überlagern, sofern sie:

- einen größeren Schutz für betroffene Personen gewährleisten, oder
- besondere Anforderungen an Gesundheitsdaten oder elektronische Gesundheitsdaten stellen.
- ONCARE und verbundene Unternehmen bekennen sich ausdrücklich zur Einhaltung aller relevanten bundesstaatlichen Gesetze, darunter u. a.:

- **California Consumer Privacy Act (CCPA/CPRA)**
- **Texas Medical Privacy Act (TMPA)**
- **New York SHIELD Act**
- **Massachusetts Data Security Regulations**
- sowie vergleichbare Datenschutzgesetze auf Landesebene

Soweit ONCARE im Auftrag von Covered Entities tätig wird, erfolgt die Verarbeitung unter Beachtung sowohl des HIPAA als auch der jeweils anwendbaren landesrechtlichen Datenschutzstandards, sofern diese strenger sind als die HIPAA-Vorgaben. Bei Abweichungen gilt stets die Regelung, die dem betroffenen Patienten **den höheren Datenschutz bietet**.

Ergänzend zu den bundesweiten HIPAA-Regelungen gelten in einzelnen Bundesstaaten – etwa Kalifornien, New York oder Texas – zusätzliche Datenschutzgesetze. Sofern diese Gesetze strengere Anforderungen stellen als HIPAA, gelten sie vorrangig. ONCARE wird in diesen Fällen das jeweils strengste anwendbare Recht beachten.

11. Ausübung von Rechten nach HIPAA (Verfahren, Identitätsprüfung, Fristen)

Nutzer mit Wohnsitz in den USA oder deren Daten durch US-Covered Entities verarbeitet werden, haben gemäß HIPAA die unter Ziffer 4 dieser Datenschutzerklärung benannten Rechte.

Zur Wahrnehmung dieser Rechte gelten folgende Regelungen:

11.1 Antragstellung

Rechte nach HIPAA können ausgeübt werden durch:

- schriftliche Anfrage per E-Mail an: **privacy@myoncare.com**
- schriftliche Anfrage über den jeweiligen Gesundheitsdienstleister (*Covered Entity*)

11.2 Identitätsverifikation

Zum Schutz der betroffenen Person wird jede Anfrage auf Rechteausübung erst nach **erfolgreicher Verifikation der Identität** bearbeitet. Mögliche Maßnahmen sind u. a.:

- Abgleich mit bei der Registrierung verwendeten Daten
- Vorlage eines gültigen Lichtbildausweises (in sicherem Upload)

- Bestätigung über den behandelnden Arzt

11.3 Bearbeitungsfristen

ONCARE bearbeitet Anfragen:

- **innerhalb von 30 Kalendertagen**, ab dem Tag des Antragseingangs,
- Verlängerung um **weitere 30 Tage** ist einmalig zulässig; der Antragsteller wird schriftlich informiert und erhält die Begründung,
- alle Anfragen und Antworten werden gemäß 45 CFR §164.530(j) **dokumentiert und archiviert**.

12. Datenverarbeitung außerhalb der Vereinigten Staaten (Offshoring / Data Localization)

In bestimmten Fällen kann die Verarbeitung von PHI im Auftrag einer US-Covered Entity **außerhalb der Vereinigten Staaten erfolgen**, insbesondere:

- durch ONCARE GmbH mit Sitz in Deutschland (EU),
- zur Bereitstellung von technischen Infrastrukturleistungen, Hosting, Support und Produktweiterentwicklung.

Diese grenzüberschreitende Verarbeitung erfolgt ausschließlich:

- auf Grundlage eines bestehenden **Business Associate Agreements** (BAA),
- mit ausdrücklicher Dokumentation im HIPAA Risk Management Plan der Covered Entity,
- mit Einhaltung der HIPAA Security Rule sowie ergänzenden **Sicherheitsmaßnahmen nach europäischem DSGVO-Standard**, insbesondere:

  → Ende-zu-Ende-Verschlüsselung (AES-256),
  → Zugriffsbeschränkung nach Need-to-Know-Prinzip,
  → Logging aller Zugriffe mit Audit-Trail,
  → Datenhaltung nur auf Servern mit physischer Zugangskontrolle und ISO 27001-Zertifizierung.

Es erfolgt **keine Speicherung von PHI auf Systemen außerhalb der USA ohne geeignete technische Schutzmaßnahmen** und vertragliche Absicherung.

13. Administrative Schutzmaßnahmen & interne Richtlinien (Administrative Safeguards)

ONCARE hat für alle US-bezogenen Dienstleistungen administrative Maßnahmen nach 45 CFR §164.308 implementiert, darunter:

- **Datenschutzverantwortliche und HIPAA-Beauftragte** auf Unternehmensebene
- **Datenschutz- und Sicherheitsrichtlinien**, versioniert, dokumentiert und durch Schulungen abgesichert
- **Pflichtschulungen für alle Mitarbeitende**, die mit US-Gesundheitsdaten arbeiten (mind. jährlich)
- **Sanktionsregelungen** bei Datenschutzverstößen im Sinne des 45 CFR §164.530(e)
- **Risikobasierte Systemprüfung und Schwachstellenanalysen**, mindestens jährlich oder bei wesentlichen Systemänderungen

Alle Prozesse sind dokumentiert in einem internen **HIPAA-Compliance-Handbuch**, das regelmäßig aktualisiert und im internen Audit überprüft wird.

14. Technische Sicherheitsmaßnahmen gemäß HIPAA Security Rule (Technical Safeguards)

ONCARE hat technische Schutzmaßnahmen gemäß 45 CFR §164.312 vollständig implementiert:

Kategorie	Maßnahme
Access Control	Rollenbasierter Zugang, eindeutige Benutzer-IDs, automatische Sitzungsabmeldung, Verfahren für den Zugang in Notfällen
Audit Controls	Vollständige System- und Zugriffprotokollierung mit regelmäßiger Auswertung

Kategorie	Maßnahme
Integrity Controls	Hash-basierte Integritätsprüfungen und Versionskontrolle bei kritischen medizinischen Daten
Authentication	Zwei-Faktor-Authentifizierung für medizinisches Personal und Administratoren
Transmission Security	TLS 1.3-Verschlüsselung bei Übertragung, VPN-Absicherung für alle externen Dienstleister

Diese Maßnahmen gelten für alle Systeme, die PHI speichern, verarbeiten oder übertragen. Die Umsetzung wird jährlich durch technische Penetrationstests und eine **HIPAA-konforme Risikoanalyse** gesichert.

***