A PARTIR DE JUNHO DE 2025

Bem-vindo ao myoncare, o portal digital de saúde e aplicativo móvel ("**Aplicação**") para atendimento eficiente e baseado nas necessidades do paciente e suporte para a gestão da saúde ocupacional.

Esta política de privacidade está dividida em duas partes:

- A primeira parte contém os regulamentos de proteção de dados para o uso da plataforma myoncare na Europa em conformidade com o **Regulamento Geral de Proteção de Dados da UE (GDPR).**

- A segunda parte contém **Informações adicionais** de acordo com os requisitos de **a Lei de Proteção de Dados dos Estados Unidos da América (HIPAA),** em particular para usuários residentes nos EUA ou no caso de processamento de dados de saúde por prestadores de serviços de saúde dos EUA.

Para nós da Oncare GmbH (doravante denominada "**ONCARE"** ou "**nós**", **"Nós**", "**nosso**"), a proteção de sua privacidade e quaisquer dados pessoais relacionados a você durante o uso do **Aplicação** é de grande importância e importância. Estamos cientes da responsabilidade que decorre da sua confiança no fornecimento e armazenamento de seus dados pessoais (de saúde) no aplicativo myoncare. Portanto, nossos sistemas de tecnologia usados para os serviços myoncare são configurados de acordo com os mais altos padrões e o processamento legal dos dados está no centro de nosso entendimento ético como empresa.

Processamos seus dados pessoais de acordo com a legislação aplicável sobre proteção de dados pessoais, em particular o Regulamento Geral de Proteção de Dados da UE (**"GDPR")** e as leis específicas do país que se aplicam a nós. Nesta política de privacidade, você aprenderá por que e como **ONCARE** Processa seus dados pessoais (de saúde) que coletamos de você ou que você nos fornece quando decide usar o Aplicativo myoncare. Em particular, você encontrará uma descrição dos dados pessoais que coletamos e processamos, bem como a finalidade e a base sobre a qual processamos os dados pessoais e os direitos aos quais você tem direito.

Leia atentamente a Política de Privacidade para a compreensão de cada item aqui disposto. Depois de ler a Política de Privacidade, você terá a oportunidade de concordar com a Política de Privacidade e consentir com o processamento de seus dados pessoais (de saúde) conforme descrito na Política de Privacidade. Se você der seu consentimento, a Política de Privacidade se tornará parte do contrato entre você e a Oncare.
De acordo com os termos de uso, nossa oferta é destinada apenas a maiores de 18 anos. Assim, nenhum dado pessoal de crianças e adolescentes menores de 18 anos é armazenado e processado.

1. DEFINIÇÕES

"**Usuário do aplicativo**" significa qualquer usuário do Aplicativo myoncare (Paciente e/ou Funcionário).

"**Blockchain**" é outro banco de dados no sistema myoncare que armazena os dados correspondentes do aplicativo.

"**Empresa**" significa seu empregador se você e seu empregador usarem as ferramentas myoncare para a gestão da saúde ocupacional do empregador.

"**Provedor de serviços de dados**" significa qualquer agente contratado e instruído pela Empresa para coletar, revisar e interpretar dados de funcionários pseudonimizados ou anônimos em programas de gestão de saúde ocupacional com base em um contrato de serviço separado com a Empresa (por exemplo, analista de dados, serviços gerais de prevenção de saúde, serviços de avaliação de dados, etc.), que é fornecido por uma folha de informações separada aos funcionários.

"**prestador de serviços de saúde**" pode ser seu médico, clínica, instituições de saúde ou outro profissional de saúde agindo por conta própria ou em nome de seu médico, clínica ou instituições de saúde.

"Pathway" é um plano de tratamento padronizado que consiste em várias care tasks, possivelmente sequenciadas no tempo, que podem determinar as etapas para diagnósticos e terapias.

"Care tasks" são tarefas ou ações específicas dentro de um percurso que devem ser realizadas pelos profissionais de saúde envolvidos, pela equipe de enfermagem ou pelo próprio paciente.

"**Aplicativo Myoncare**" significa o aplicativo móvel myoncare para uso por pacientes ou funcionários que desejam usar os serviços oferecidos pela ONCARE.

"**Portal myoncare**" é o portal da web myoncare, que se destina ao uso profissional dos usuários do portal e serve como uma interface entre os usuários do portal e os usuários do aplicativo.

"**Ferramentas myoncare**" significa o Aplicativo myoncare e o Portal myoncare juntos.

"**myoncare PWA**" significa o aplicativo myoncare Progressive Web App para pacientes que desejam usar os serviços oferecidos pela Oncare pelo PWA e não pelo aplicativo myoncare.

"**Serviços myoncare**" significa os serviços, funcionalidades e outras ofertas que são ou podem ser oferecidas aos Usuários do Portal por meio do portal myoncare e/ou aos usuários do aplicativo por meio do Aplicativo myoncare.

"**ONCARE"** significa ONCARE GmbH, Alemanha.

"**Usuário do portal**" significa qualquer prestador de serviços de saúde, empresa ou provedor de serviços de dados que usa o Portal myoncare baseado na web.

"**Política de privacidade**" significa esta declaração dada a você como paciente e usuário do Aplicativo myoncare, que descreve como coletamos, usamos e armazenamos suas informações pessoais e informa sobre seus amplos direitos.

"**Termos de Uso**" significa os termos de uso para o uso do Aplicativo myoncare.

2. PROCESSAMENTO DE DADOS DE (TRATAMENTO)

A Oncare GmbH, uma empresa registrada no Tribunal Distrital de Munique sob o número de registro 219909 com sede em Balanstraße 71a, 81541 Munique, Alemanha, oferece o aplicativo móvel **Aplicativo myoncare** e o opera como acesso ao **Serviços myoncare**. Este **política de privacidade** se aplica a todos os dados pessoais processados pela ONCARE em conexão com o uso do **Aplicativo Myoncare** .

3. O QUE SÃO DADOS PESSOAIS

"**dados pessoais**" significa qualquer informação que permita identificar uma pessoa singular. Em particular, isso inclui seu nome, aniversário, endereço, número de telefone, endereço de e-mail e endereço IP.

"**Dados de saúde**" significa dados pessoais relacionados à saúde física e mental de uma pessoa física, incluindo a prestação de serviços de saúde que divulgam informações sobre seu estado de saúde.

Os dados devem ser considerados "**anônimo**" se nenhuma conexão pessoal com a pessoa/usuário puder ser estabelecida.
Em contraste, dados "**pseudônimos**" são dados a partir dos quais uma referência pessoal ou informação de identificação pessoal é substituída por um ou mais identificadores artificiais ou pseudónimos, mas que geralmente podem ser reidentificados pela chave identificadora.

4. PWA myoncare
Um aplicativo da web progressivo (PWA) é um site que parece e tem a funcionalidade de um aplicativo móvel. Os PWAs são criados para aproveitar os recursos nativos dos dispositivos móveis sem a necessidade de uma loja de aplicativos. O objetivo dos PWAs é combinar a diferença entre aplicativos e a web tradicional, trazendo os benefícios dos aplicativos móveis nativos para o navegador. O PWA é baseado na tecnologia de "React". "React" é um software de código aberto para aplicativos PWA.

Para usar o **myoncare PWA**, os pacientes precisam de um computador ou smartphone e uma conexão ativa com a Internet. Não há necessidade de baixar um aplicativo.

As seguintes informações sobre o **Aplicativo Myoncare** também se aplica ao **myoncare PWA**, salvo disposição em contrário nesta secção.

5. QUAIS DADOS PESSOAIS SÃO USADOS AO USAR O APLICATIVO MYONCARE

Podemos processar as seguintes categorias de dados sobre você ao usar o **Aplicativo Myoncare** :

Dados operacionais: Dados pessoais que você nos fornece ao se registrar em nosso **Aplicativo Myoncare**, entrando em contato conosco sobre problemas com o aplicativo ou interagindo conosco com a finalidade de usar o aplicativo**.**

Dados de tratamento: Você ou seu médico nos fornecem seus dados pessoais, como nome, idade, altura, peso, indicação, sintomas de doença e outras informações relacionadas ao seu tratamento (por exemplo, em um care plan). As informações relacionadas ao seu tratamento incluem, mas não se limitam a: informações sobre medicamentos tomados, respostas a questionários, incluindo informações relacionadas a doenças ou condições, diagnósticos e terapias fornecidas por seu **prestador de serviço de saúde** , tarefas planejadas e concluídas.

Dados da loja comercial: Dados da Loja Comercial: Dados pessoais processados em conexão com o uso da Loja myoncare – em particular em conexão com a autoria, configuração ou compra de planos de tratamento digital ("Pathways"). A loja é operada pela myon.clinic GmbH, uma subsidiária da Oncare GmbH. O uso da Loja requer o processamento de seu nome, detalhes de contato profissional e, se aplicável, dados de pagamento (somente para conteúdo pago). A Oncare GmbH processa esses dados exclusivamente para o fornecimento técnico das funções da plataforma e não para seus próprios fins comerciais.

Dados de atividade: Dados pessoais que são processados por nós se você conectar o **Aplicativo Myoncare** em um aplicativo de saúde (por exemplo, GoogleFit, AppleHealth, Withings). Seus dados de atividade serão transferidos para seu afiliado **prestadores de serviços** como **usuários do portal** .

Dados de pesquisa comercial e não comercial:
Processamos seus dados pessoais de forma anônima/pseudonimizada para analisar e produzir relatórios científicos resumidos para melhorar produtos, tratamentos e resultados científicos.

Uso de dados anônimos para fins comerciais: Além disso, a ONCARE pode usar certos dados de saúde e uso, uma vez totalmente anonimizados, para fins comerciais – como melhorar a plataforma, analisar processos de atendimento ou desenvolver novos serviços de saúde digital. A anonimização é realizada de forma que os indivíduos não possam mais ser identificados. Esses dados anônimos não estão mais sujeitos ao GDPR.

Dados de fabricantes de dispositivos, distribuidores de dispositivos médicos ou laboratórios:
Além disso, os dados pessoais podem ser processados por fabricantes de dispositivos médicos conectados, distribuidores de dispositivos médicos ou prestadores de serviços laboratoriais como parte de processos de atendimento integrados, desde que sejam comissionados ou usados pelo prestador de serviços por meio do portal myoncare.

Dados de segurança do produto: Dados pessoais que são processados para cumprir nossas obrigações legais como fabricante do **Aplicativo Myoncare** como um dispositivo médico. Além disso, seus dados pessoais podem ser processados por empresas de dispositivos médicos ou farmacêuticas para fins de segurança legal ou vigilância.

Dados de reembolso: Dados pessoais necessários para o processo de reembolso entre seu provedor e seu provedor de seguro de saúde.

Dados de gestão de saúde ocupacional: Dados pessoais ou agregados coletados em projetos e questionários específicos a pedido da sua **empresa** (diretamente ou por meio de um provedor de serviços de dados contratado por sua empresa). Os dados podem estar relacionados a determinadas informações de saúde, sua opinião sobre seu bem-estar pessoal, sua opinião como funcionário sobre uma determinada situação interna ou externa ou dados sobre cuidados ou saúde em geral.

6. TECNOLOGIA BLOCKCHAIN

Tecnologia **Blockchain** ("**Blockchain**") (Patente Europeia n.º 4 002 787) é um serviço opcional que não é obrigatório. É o seu **fornecedor de serviços** que decide usar a solução blockchain. O **blockchain** é baseado na tecnologia do Hyperledger Fabric. O Hyperledger Fabric é um software de código aberto para implementações de blockchain de nível empresarial. Ele oferece uma plataforma escalável e segura que dá suporte a projetos de blockchain.

O blockchain no sistema myoncare é um banco de dados adicional que armazena dados do aplicativo. Todos os dados do blockchain são armazenados na República Federal da Alemanha. É um privado **blockchain** ("**Blockchain Privado**"), ele só permite a entrada de participantes verificados selecionados e é possível substituir, editar ou excluir entradas conforme necessário.

Geralmente, o **blockchain** consiste em dados digitais em uma cadeia de pacotes chamados "blocos" que armazenam as transações correspondentes. A maneira como esses blocos estão conectados uns aos outros é cronológica. O primeiro bloco criado é chamado de bloco de gênese, e cada bloco adicionado depois disso tem um hash criptográfico relacionado ao bloco anterior, de modo que as transações e alterações de informações podem ser rastreadas até o bloco de gênese. Todas as transações dentro dos blocos são validadas e verificadas por meio de um mecanismo de consenso blockchain para garantir que cada transação seja inalterada.

Cada bloco contém a lista de transações, um carimbo de data/hora, seu próprio hash e o hash do bloco anterior. Um hash é uma função que converte dados digitais em uma cadeia alfanumérica. Se uma pessoa não autorizada tentar alterar os dados de um único bloco, o hash do bloco também seria alterado e o link para esse bloco seria perdido. Nesse caso, o bloco não pode mais ser sincronizado com os demais. Este processo técnico impede que pessoas não autorizadas manipulem o conteúdo do **blockchain** cadeia. Quando todos os nós (nós de rede) tentam sincronizar suas cópias, ele detecta que uma cópia foi modificada e a rede considera esse nó não íntegro.

Nosso **blockchain** é um privado **blockchain**. Um privado **blockchain** é descentralizado. Este é o chamado sistema de contabilidade distribuída que atua como um banco de dados fechado. Ao contrário do público **Blockchains**, que são "não autorizados", privados **Blockchains** são "autorizados" porque a autorização é necessária para se tornar um usuário. Ao contrário do público **Blockchains**, acessíveis ao público por todos, o acesso a **Blockchains** depende da elegibilidade para se tornar um usuário. Essa estrutura permite aproveitar a segurança e a imutabilidade da tecnologia blockchain, ao mesmo tempo em que está em conformidade com a proteção de dados e, em particular, com os regulamentos do Regulamento Geral de Proteção de Dados (GDPR). Os registros privados de blockchain podem ser editados, modificados ou excluídos. Nesse contexto, a exclusão significa que o valor de referência ao UUID (Identificador Universalmente Exclusivo) no serviço **provedor de** banco de dados é excluído. Além disso, o hash é anonimizado no banco de dados blockchain, para que esse processo geral esteja em conformidade com o Regulamento Geral de Proteção de Dados e os direitos de um titular de dados sejam garantidos (direito ao apagamento/"direito de ser esquecido", Art. 17 do RGPD).

Tipo de dados armazenados e processados em blockchain:

- Instituições/**Leistungserbinger** UUID
- UUID do paciente
- UUID do ativo
- Hash de caretask e dados de ativos. (UUID: Identificador Único Universal).

Os arquivos armazenados no arquivo **blockchain** são pseudo-anonimizados.

Nosso **blockchain** foi projetado para garantir a privacidade dos dados em termos de integridade de dados, perfil do paciente, ativos e atribuídos **care tasks** e medicamentos. Para se comunicar com o **blockchain**, o usuário deve registrar uma série de chaves público-privadas. Para se comunicar com o **blockchain**, o usuário precisa de várias chaves público-privadas; O processo de registro gera certificados que são armazenados em um banco de dados separado do **provedor** e no celular do paciente. Uma cópia de backup da chave do paciente é criptografada e armazenada no **provedor**, que só pode ser acessado pelo paciente.

Ao verificar o consentimento para a proteção de dados, caso o **Provedor** deseja se comunicar com o Paciente, o sistema verifica se o Paciente deu consentimento à Política de Privacidade do Provedor. O **blockchain** portanto, serve para garantir a integridade e responsabilidade do registro para garantir que o paciente tenha aceitado a política de privacidade.

Quando um **prestador de serviço de saúde** carrega uma nova versão de uma política de privacidade, o hash do arquivo é armazenado no **blockchain,** e depois que o paciente concorda com a política de privacidade, essa interação é armazenada no **blockchain** . Toda vez que o paciente se comunica, o **blockchain** responde comparando o hash com um sinalizador que indica se o consentimento do paciente ainda é válido para a política de privacidade atual.

A integridade do perfil do paciente também é garantida pelo blockchain na sincronização do paciente. O **prestador de serviço de saúde** detecta imediatamente se o perfil do paciente não está sincronizado ou corresponde ao perfil no celular, comparando o hash do perfil do paciente no **blockchain**. Desta forma, o **provedor de serviços alcança** atualização suficiente em relação ao perfil do paciente.

Portal myoncare:
Se o **fornecedor de serviços** escolher a solução blockchain, a ONCARE implementa uma ferramenta adicional, denominada "Adapter Service", que é utilizada para comunicar com o **blockchain** . A instância blockchain é hospedada pela ONCARE.

Aplicativo Myoncare:
Os pacientes podem se conectar à mesma instância de blockchain usando a ferramenta Phone Manager, que também é hospedada pela ONCARE. Este serviço também é hospedado pela ONCARE.

Base legal para o processamento de dados: Tratamento de dados pela ONCARE em nome da **Fornecedor de serviços** é realizado com base no Art. 28 GDPR (Contrato de Processamento de Dados).

7. TRATAMENTO DE DADOS OPERACIONAIS

Aplicável a todos os usuários do aplicativo

Você pode nos fornecer certos dados pessoais ao entrar em contato conosco para entender as funções e o uso do **Aplicativo Myoncare** , no caso de uma solicitação de serviço sua ou no caso de uma oferta de suporte iniciada por nós (por telefone).

Funcionários de serviço
Em nome do controlador de dados (por exemplo, oferecemos suporte no preenchimento de questionários por telefone (chamadas de saída) para otimizar o atendimento digital ao paciente. Se você não quiser aproveitar esta oferta, você é livre para não aceitá-la e se opor ao suporte por telefone.

No caso de uma solicitação de serviço e uma chamada de saída, os seguintes dados pessoais também podem ser visualizados por funcionários autorizados da ONCARE:

- Os dados pessoais que você forneceu ao seu **fornecedor de serviços** através do nosso aplicativo (por exemplo, nome, data de nascimento, foto do perfil, detalhes de contato).

- Os dados de saúde que você forneceu ao seu **Médico** dados **fornecedor de serviços** ou **empregador** através do nosso **Aplicativo Myoncare** (por exemplo, informações sobre medicamentos tomados, respostas a questionários, incluindo informações relacionadas a doenças ou condições, diagnósticos e terapias de profissionais de saúde, tarefas planejadas e concluídas).

Funcionários autorizados da ONCARE que podem acessar o banco de dados do seu provedor de serviços**,** Provedor de serviços de dados **ou** empregador **para fins de processamento de uma solicitação de serviço ou de uma chamada de saída** são contratualmente obrigados a manter todos os dados pessoais estritamente confidenciais.

Notificações push e e-mails
Como parte do seu apoio do myoncare, gostaríamos de informá-lo sobre como lidamos com notificações e informações importantes que enviamos a você.

1. **Notificações push**:
   - Enviamos notificações push por meio de nosso **myoncare PWA** (WebApp Progressivo) e **O aplicativo myoncare** para informá-lo sobre tarefas, compromissos e atualizações importantes.
   - Você tem a opção de desativar essas notificações push nas configurações do seu aplicativo.
2. **Notificações por e-mail**:
   - Se você ativou ou desativou as notificações push, continuaremos a enviar informações e lembretes importantes por e-mail.
   - Isso garante que você não perca nenhuma notificação importante e que seu suporte funcione sem problemas.

Por que fazemos isso:
- Nosso objetivo é mantê-lo atualizado com suas tarefas e atualizações importantes para apoiar sua saúde da melhor maneira possível.
- Os e-mails são uma maneira confiável de garantir que informações importantes cheguem até você, mesmo quando as notificações push estão desativadas.

Suas opções de ação:
- Se você não quiser receber notificações push, poderá desativá-las nas configurações do aplicativo myoncare.
- Certifique-se de que seu endereço de e-mail esteja correto e atualizado para garantir uma recepção tranquila de nossas mensagens.
- Se você não quiser receber lembretes por e-mail, poderá desativá-los nas configurações do aplicativo myoncare.

Período de armazenamento
Os dados que você nos fornece para receber e-mails serão armazenados por nós até que você saia de nossos serviços e serão excluídos de nossos servidores e dos servidores do Sendgrid após o logout.

Ao processar dados operacionais, a ONCARE atua como controladora de dados responsável pelo processamento legal de seus dados pessoais.

Tipos de dados: seu nome, endereço de e-mail, número de telefone, data de nascimento, data de registro, pseudo-chaves geradas pelo aplicativo; Tokens de dispositivo para identificar seu dispositivo, seu número de pseudo-identificação, seu endereço IP, tipo e versão do sistema operacional usado pelo seu dispositivo.

Quando o **Aplicativo Myoncare** for baixado, as informações necessárias serão transmitidas ao provedor da loja de aplicativos. Não temos influência sobre essa coleta de dados e não somos responsáveis por ela. Processamos os dados pessoais que nos são fornecidos pelo fornecedor da loja de aplicações no âmbito da nossa relação contratual com o objetivo de desenvolver ainda mais a nossa **Aplicativos Myoncare** e serviços.

O aplicativo usa a API do Google Maps para usar informações geográficas. Ao usar o Google Maps, o Google também coleta, processa e usa dados sobre o uso das funções do mapa. Você pode encontrar mais informações sobre o escopo, a base legal e a finalidade do processamento de dados pelo Google, bem como o período de armazenamento, na política de privacidade do Google.

Finalidades do processamento de dados operacionais: Usamos os dados operacionais para manter as funcionalidades do **Aplicativo Myoncare** e para entrar em contato diretamente com você, se necessário ou iniciado por você (por exemplo, em caso de alterações nos termos e condições gerais, suporte necessário, problemas técnicos, assistência no preenchimento dos questionários, etc.).

Justificação do tratamento: O tratamento de dados da empresa é justificado com base no art. 6 (1) (b) GDPR para a execução do contrato que você celebra com a ONCARE com a finalidade de usar o **Aplicativo Myoncare** .

8. GEOLOCALIZAÇÃO IP

Usamos um aplicativo de geolocalização para nossos serviços. Usamos ipapi (fornecido pela apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Viena, Áustria) e Geoapificar (fornecido pela Keptago Ltd., N. Nikolaidi e T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Chipre) para identificar a localização dos usuários pacientes. Nós os usamos para proteger nossos aplicativos e verificar a localização do usuário paciente para garantir que o uso de nossos serviços seja compatível. Não combinamos as informações que coletamos com outras informações sobre o usuário que possam identificá-lo. Os dados processados pelo apilayer incluem o endereço IP do paciente e outras informações de localização. A base legal para o uso é o Art. 6 par. 1 lit. f RGPD. Os dados serão excluídos quando a finalidade para a qual foram coletados não existir mais e não houver mais obrigação legal de retê-los. Para obter mais informações sobre suas políticas de privacidade, visite https://ipapi.com/privacy/

9. PROCESSAMENTO DE DADOS DE (TRATAMENTO)

Aplicável a usuários do aplicativo que usam o aplicativo com seu provedor de serviços.

Ao usar o **Aplicativo Myoncare**teu **fornecedor de serviços** pode inserir seus dados pessoais no **Portal myoncare** para iniciar o **Serviços myoncare** (por exemplo, criá-lo como paciente, provisão de uma tarefa individual, lembrete para tomar medicamentos, etc.). Além disso, você e seu **fornecedor de serviços pode fazer upload** documentos e arquivos ao **Aplicativo Myoncare** e o **Portal myoncare** e compartilhá-los uns com os outros. Seu **provedor** pode fazer upload de um **política de privacidade** para sua informação e definir outros requisitos de consentimento para você como paciente para os quais seu consentimento é necessário. Os arquivos são armazenados em um banco de dados em nuvem na Alemanha. Seu **fornecedor de serviços** pode permitir o compartilhamento de tais arquivos com outros **Usuários do portal** dentro de sua instituição ou de outra **Prestadores de serviços** fora das suas instalações (médicos consultores) para fins médicos. Outros usuários do portal não terão acesso a esses arquivos sem esse compartilhamento. Além disso, seu **fornecedor de serviços** pode nos instruir a ajudá-lo por telefone no preenchimento de questionários (chamadas de saída). Isso é feito apenas de acordo com as instruções do seu provedor de serviços e é realizado exclusivamente por funcionários autorizados da ONCARE.

Usaremos e processaremos seus dados de acordo com os **termos estabelecidos nesta Política de Privacidade**, desde que você nos dê seu consentimento quando necessário.

Processamos esses dados pessoais, incluindo seus dados de saúde, sob um contrato e de acordo com as instruções do seu **prestador de serviço de saúde**. Para esses fins de processamento, o **fornecedor de serviços** é responsável pelo processamento de seus dados pessoais e dados de saúde como controlador de dados de acordo com as leis de proteção de dados aplicáveis, e a ONCARE é a processadora de dados desses dados pessoais (de saúde). Isso significa que a ONCARE processa dados pessoais apenas de acordo com as instruções do **fornecedor de serviços**. Se você tiver alguma dúvida ou preocupação sobre o processamento de seus dados pessoais ou dados de saúde, entre em contato com seu prestador de serviço de saúde em primeiro lugar .

Tipos de dados: nome, data de nascimento, informações de perfil, detalhes de contato e também dados de saúde, como sintomas, fotos, informações sobre medicamentos tomados, respostas a questionários, incluindo informações relacionadas a doenças ou condições, diagnósticos e terapias por profissionais de saúde, tarefas planejadas e concluídas.

Finalidades do processamento de dados: Processamos seus dados de tratamento para fornecer nossos **Serviço myoncare** para o seu **fornecedor de serviços** e para você. Seus dados de saúde, que você insere em nosso **Aplicativo Myoncare** , será usado pelo seu **fornecedor de serviços** para aconselhamento e apoio para você. Processamos esses dados pessoais sob um contrato e de acordo com as instruções do seu **fornecedor de serviços**. A transmissão desses dados de tratamento é pseudonimizada e criptografada. Para exercer seus direitos como titular dos dados, entre em contato com seu **Prestadores de serviços**.

Justificação do tratamento dos dados de tratamento: Seus dados pessoais (tratamento) serão processados pelo seu **fornecedor de serviços** de acordo com as disposições do **RGPD** e todos os outros regulamentos de proteção de dados aplicáveis. As bases legais para o processamento de dados resultam, em particular, do Art. 9 (2) (h) GDPR para dados de saúde como dados particularmente sensíveis, bem como seu consentimento de acordo com o Art. 6 (1) (a) e 9 (2) (a) GDPR. O tratamento de dados pela ONCARE para seus **Prestadores de serviços** também é realizado com base no art. 28 GDPR (Contrato de Processamento de Dados).
Seu **fornecedor de serviços** é responsável por obter seu consentimento como controlador de dados. Mesmo que você possa usar o **Aplicativo Myoncare** Sem esse consentimento, a maioria das funções não funcionará mais (por exemplo, compartilhamento de dados com seu médico). A recusa ou revogação do consentimento para o processamento de dados de tratamento leva, portanto, a uma restrição severa da funcionalidade dos serviços do aplicativo e do seu **Prestadores de serviços** não pode mais apoiá-lo através do **Aplicativo Myoncare**.

10. PROCESSAMENTO DE DADOS DE ATIVIDADE

Aplicável apenas se você concordar e ativar a transferência de dados de atividade por meio das ferramentas myoncare.

Ferramentas myoncare oferecer-lhe a opção de conectar o **Aplicativo Myoncare** com determinados aplicativos de saúde (por exemplo, AppleHealth, GoogleFit, Withings) que você usa ("**Aplicativo Saúde**"). Para permitir o processamento de dados de atividade, obtemos seu consentimento para o processamento com antecedência. Se a conexão for estabelecida após o seu consentimento, o **Dados de atividade coletados** pelo **Aplicativo Saúde** serão disponibilizados aos seus provedores para fornecer informações contextuais adicionais sobre sua atividade. Observe que os dados da atividade não são validados por **Ferramentas myoncare** e não deve ser usado pelo seu **prestador de serviço de saúde** para fins de diagnóstico como base para a tomada de decisões médicas. Observe também que seu **Provedores** não são obrigados a verificar seus dados de atividade e não precisam fornecer feedback sobre seus dados de atividade.

Os dados da atividade são compartilhados **com seu prestadores de serviços** afiliado toda vez que o **Aplicativo Myoncare** é acessado. Você pode revogar seu consentimento para a divulgação de dados de atividade a qualquer momento nas configurações do **Aplicativo Myoncare**. Observe que seus dados de atividade não serão mais compartilhados a partir deste ponto. Os dados de atividade que já foram compartilhados não serão excluídos do **Portal myoncare** do seu afiliado **Prestadores de serviços**.

O processamento de dados de atividade é de sua própria responsabilidade.

Tipos de dados: O tipo e a quantidade de dados transferidos dependem da sua decisão e da disponibilidade desses dados dentro do **Aplicativo Saúde** . Os dados podem incluir peso, altura, passos dados, calorias queimadas, horas de sono, frequência cardíaca e pressão arterial, entre outros.

Finalidade do processamento de dados da atividade: Seus Dados de Atividade serão fornecidos ao seu Afiliado **Provedores** para fornecer informações contextuais adicionais sobre sua Atividade.

Justificativa do processamento: O processamento dos Dados de Atividade é feito sob sua própria responsabilidade.

11. PROCESSAMENTO DE DADOS DE SEGURANÇA DO PRODUTO

Aplicável a usuários de aplicativos cujo provedor de serviços usa a variante de dispositivo médico das ferramentas myoncare.

O **Aplicativo Myoncare** é classificado e comercializado como um dispositivo médico de acordo com os Regulamentos Europeus de Dispositivos Médicos. Como fabricante do aplicativo, temos que cumprir certas obrigações legais (por exemplo, monitorar a funcionalidade do aplicativo, avaliar relatórios de incidentes que possam estar relacionados ao uso do aplicativo, rastrear usuários, etc.). Além disso, o **Aplicativo Myoncare** permite que você e seu **Médico** para comunicar e coletar informações pessoais sobre dispositivos médicos ou medicamentos específicos usados em seu tratamento. Os fabricantes desses dispositivos médicos ou medicamentos também têm obrigações legais no que diz respeito à fiscalização do mercado (por exemplo, recolha e avaliação de relatórios de efeitos secundários).

A ONCARE é a controladora de dados para o processamento de dados de segurança do produto.

Tipos de dados: Relatos de casos, dados pessoais fornecidos em um relatório de incidente e resultados da avaliação.

Processamento de dados de segurança do produto: Armazenamos e avaliamos todos os dados pessoais em conexão com nossas obrigações legais como fabricante de um dispositivo médico e transmitimos esses dados pessoais (na medida do possível após a pseudonimização) para autoridades competentes, órgãos notificados ou outros controladores de dados com funções de supervisão. Além disso, armazenaremos e transferiremos dados pessoais relacionados a dispositivos médicos e/ou medicamentos se recebermos avisos de seu **Prestador de serviços de saúde**, de si na qualidade de doente ou de terceiros (por exemplo, os nossos distribuidores ou importadores do **Ferramentas myoncare** em seu país) que devem ser relatados ao fabricante do produto para que o fabricante cumpra suas obrigações legais sobre segurança do produto .

Justificação do tratamento dos dados de segurança dos produtos: A base legal para o processamento de dados pessoais para o cumprimento de obrigações legais como fabricante de dispositivos médicos ou farmacêuticos é o Art. 6 (1) (c), Art. 9 (2) (i) GDPR em conjunto com as obrigações de monitoramento pós-comercialização sob a Lei de Dispositivos Médicos e a Diretiva de Dispositivos Médicos (regulamentada a partir de 26 de maio de 2021 no Capítulo VII do novo Regulamento de Dispositivos Médicos (UE) 2017/745) e/ou a Lei de Medicamentos.

Complemento à exclusão de responsabilidade por efeitos secundários:
A Oncare GmbH não realiza nenhuma avaliação médica do conteúdo transmitido e não é obrigada a encaminhar informações relevantes para a legislação farmacêutica, como efeitos colaterais, erros de aplicação ou defeitos do produto às autoridades. Esta responsabilidade é exclusivamente dos prestadores de serviços de tratamento ou, se afetados, dos respetivos fabricantes dos produtos utilizados.

12. TRATAMENTO DE DADOS RELATIVOS À SAÚDE E AO TRATAMENTO

Aplicável a usuários do aplicativo que usam o aplicativo com seu provedor de serviços para fins de reembolso.
O **Aplicativo Myoncare** suporta seu **prestador de serviço de saúde** ao iniciar procedimentos padrão para reembolso de custos dos serviços de saúde prestados a você por meio do **Aplicativo Myoncare**. Para viabilizar o processo de reembolso, o **Aplicativo Myoncare** apoia a recolha dos seus dados pessoais (de saúde) pelo seu **fornecedor de serviços** para efeitos de transmissão destes dados à sua entidade pagadora (a Associação dos Médicos Estatutários de Seguros de Saúde e/ou a sua companhia de seguros de saúde). Este processamento de dados é apenas uma transferência de dados inicial para o **fornecedor de serviços** para obter o reembolso da sua companhia de seguros de saúde. O tipo e a quantidade de dados pessoais tratados não diferem de outras rotinas de reembolso do **Fornecedor de serviços**. Seu provedor de serviços é o Controlador de Dados para Dados de Reembolso. A ONCARE atua como processador de dados com base no contrato de processamento de dados com seu **fornecedor de serviços**.

Tipos de dados: nome, diagnóstico, indicações, tratamento, duração do tratamento, outros dados necessários para a gestão do reembolso.

Processamento de dados de reembolso: Seu **provedor** transmite os dados de tratamento necessários para o reembolso ao ordenante (quer à sua instituição legal de seguro de saúde e/ou à sua companhia de seguros de doença), e o ordenante processa os dados de reembolso a fim de reembolsar o seu **provedor** .

Justificação do tratamento dos dados relativos ao reembolso: Os dados de reembolso são processados com base nos §§ 295, 301 SGB V, Art. 9 par. 2 lit. b GDPR. Processamento de dados pela ONCARE para o seu **fornecedor de serviços** também é realizado com base no art. 28 GDPR (contrato de processamento de pedidos).

13. PROCESSAMENTO POR FABRICANTES DE DISPOSITIVOS, DISTRIBUIDORES DE DISPOSITIVOS MÉDICOS E PRESTADORES DE SERVIÇOS LABORATORIAIS

Se você usar funções médicas adicionais, como diagnóstico integrado, coleta de sinais vitais ou serviços laboratoriais por meio da Plataforma, os dados pessoais de saúde poderão ser coletados e processados por fornecedores terceirizados externos (por exemplo, fabricantes de dispositivos médicos, distribuidores desses ou prestadores de serviços de laboratório). Isso é feito para apoiar os cuidados médicos e sempre com base no consentimento explícito ou em uma relação de tratamento.
O processamento é realizado no âmbito do processamento de pedidos ou – dependendo do provedor – sob sua própria responsabilidade sob a lei de proteção de dados. A Oncare GmbH fornece apenas a conexão técnica para esse fim, sem verificar ou avaliar clinicamente o conteúdo. Mais informações sobre o respectivo processamento de dados podem ser obtidas diretamente com o prestador de serviços de tratamento ou por meio das informações de proteção de dados dos provedores terceirizados integrados.

14. GERENCIAMENTO DE ARMAZENAMENTO COMERCIAL DE DADOS E PATHWAY

O portal myoncare oferece aos prestadores de serviços registrados (por exemplo, médicos) a oportunidade de oferecer e configurar care pathways digital por meio de uma funcionalidade de loja virtual (por exemplo, em cooperação com myon.clinic) e atribuir pacientes individualmente.
Como parte do uso dessa funcionalidade, dados pessoais – em particular dados de saúde – são processados, como informações sobre indicação, duração recomendada do tratamento ou atribuição de pathway. Este processamento de dados serve para a individualização e atribuição de conteúdo médico e é realizado com base no Art. 6 (1) (b) e Art. 9 (2) (h) GDPR.

A Oncare fornece a infraestrutura técnica e processa os dados em questão como controladora de dados na acepção do Art. 4 No. 7 GDPR, na medida em que o processamento seja necessário para o fornecimento das funções da plataforma. No entanto, a seleção do conteúdo e o design médico dos caminhos são de responsabilidade exclusiva do respectivo provedor de serviços.
Na medida em que o faturamento ou a transmissão de dados são realizados a terceiros (por exemplo, escritórios de faturamento ou parceiros de plataforma, como myon.clinic), esse processamento ocorre apenas com base em acordos ou regulamentos legais correspondentes.

15. TRATAMENTO DE DADOS DE GESTÃO DE SAÚDE OCUPACIONAL

Aplicável aos usuários do aplicativo que usam o aplicativo com a gestão de saúde ocupacional da empresa.

Durante o uso do **Aplicativo Myoncare** na **empresa de** gestão da saúde ocupacional, certos dados pessoais (de saúde) são transmitidos de forma agregada como dados para a gestão da saúde ocupacional para a **empresa** e o **Provedores de serviços de dados** encomendado pela **empresa** (por exemplo, analistas de dados ou empresas de pesquisa). Nem a **empresa** nem qualquer **Provedor de serviços de dados** pode atribuir esses dados à sua identidade. A ONCARE recomenda **que você não compartilhe nenhum dado pessoal** ao usar os serviços myoncare como parte da gestão de saúde ocupacional.

Isso significa que o ONCARE e todos **Provedores de serviços de dados** apenas processará os dados para a gestão da saúde ocupacional de acordo com as instruções **da empresa** . Processamos esses dados para gerenciamento de saúde ocupacional, incluindo seus dados de saúde, com base em um acordo com sua **empresa** e/ou um **Provedor de serviços de dados** e de acordo com suas instruções. Para efeitos do presente acordo, entende-se por: **empresa** ou o **Provedor de dados** é o responsável pelo tratamento dos seus dados para fins de gestão da saúde ocupacional e ONCARE e quaisquer **Provedores de dados** engajado pela **empresa** são os processadores de dados de tais dados. Se você tiver alguma dúvida ou preocupação sobre o processamento de seus dados para gerenciamento de saúde ocupacional, entre em contato com a empresa em primeiro lugar **.**

Finalidades do tratamento de dados na gestão da saúde ocupacional: Processamos seus dados para gestão de saúde ocupacional, a fim de poder oferecer a você e à **empresa** nossos **Serviços myoncare**. Seus dados de gestão de saúde ocupacional, que você insere em nosso **Aplicativo Myoncare**, será usado pelo **empresa** (diretamente ou através de um **Provedor de dados**) como parte da gestão da saúde do trabalhador. Processamos esses dados para gestão de saúde ocupacional no âmbito de um acordo com e de acordo com as instruções da **empresa** e/ou um **Provedor de dados** para sua gestão em saúde ocupacional. A transmissão desses dados para a gestão da saúde ocupacional é pseudonimizada e criptografada. Para exercer seus direitos como titular dos dados, entre em contato com a **Empresa**.

Justificação do processamento dos dados de gestão da saúde no trabalho: Seus dados de gestão de saúde ocupacional serão processados pela **Empresa** de acordo com as disposições do **GDPR** e todos os outros regulamentos de proteção de dados aplicáveis. A base legal para o processamento de dados é, em particular, o seu consentimento de acordo com o Art. 6 (1) (a) e Art. 9 (2) (a) um GDPR ou outra base legal aplicável à **Empresa**. O tratamento de dados pela ONCARE em nome da **Empresa** (diretamente ou por meio de um prestador de serviços contratado por sua Empresa) também é baseado no Art. 28 GDPR (Contrato de Processamento de Dados).
A **Empresa** , como controladora de dados, é responsável por obter seu consentimento quando exigido pelos regulamentos de proteção de dados e processar os dados para fins de gerenciamento de saúde ocupacional de acordo com as leis de proteção de dados aplicáveis.

16. QUAL TECNOLOGIA É USADA PELO APLICATIVO MYONCARE?

Serviço de e-mail
Usamos Brevo (fornecido pela Sendinblue GmbH, localizada na Köpenicker Straße 126, 10179 Berlim) e Sendgrid (fornecido pela Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, EUA). Esses serviços de e-mail podem ser usados para organizar o envio de e-mails. O Sendgrid é usado para enviar e-mails de confirmação, confirmações de transações e e-mails com informações importantes sobre solicitações. Os dados que você inserir com a finalidade de receber e-mails serão armazenados nos servidores do Sendgrid. Quando enviamos e-mails em seu nome por meio do SendGrid, usamos uma conexão segura SSL.

A comunicação por e-mail é usada para as seguintes tarefas:

- Fazer login no aplicativo da web pela primeira vez;
- redefinindo a senha do aplicativo da web;

- Crie uma conta para o aplicativo do paciente;
- Redefina a senha do aplicativo do paciente;
- Elaboração e envio de relatório;
- Substitua as notificações push por e-mails para **PWA** (Progressive Web App) nos seguintes casos:
  → se um care plan termina em uma hora;
  → se a medicação foi atribuída;
  → se a Política de Privacidade foi atualizada;
  → quando é enviada uma consulta a doentes e médicos, nomeadamente para o tipo de consulta por "videochamada";
  → Qualquer informação relacionada a um **caretask** ou se um **provedor** atribuiu **um** caretask.

Brevo (Política de Privacidade):
Política de Privacidade - Proteção de Dados Pessoais | Brevo

SendGrid (Política de Privacidade):
SendGrid (Política de Privacidade): https://Sendgrid.com/resource/general-data-protection-regulation-2/

Matomo
Esta é uma ferramenta open-source de análise da Web. O Matomo (fornecido pela InnoCraft Ltd., Nova Zelândia) não transmite dados para servidores que estão fora do controle da ONCARE. O Matomo é inicialmente desativado quando você usa nossos serviços. Somente se você concordar com isso, seu comportamento de usuário será registrado anonimamente. Se isso estiver desativado, um "cookie persistente" será armazenado, se as configurações do seu navegador permitirem. Este cookie sinaliza ao Matomo que você não deseja que seu navegador seja gravado.
As informações de uso coletadas pelo cookie são transmitidas aos nossos servidores e armazenadas lá para que possamos analisar o comportamento do usuário.
As informações geradas pelo cookie sobre o seu uso são:

- Função;
- geolocalização do usuário;
- Sistema operacional do usuário;
- tempo que o usuário usou o conteúdo;
- -Endereço IP;
- Sites visitados via web/ **PWA** (para obter mais informações, consulte a seção sobre PWA nesta Política de Privacidade);
- Botões nos quais o usuário **clica no** Portal myoncare**, o** Aplicativo Myoncare **e o** myoncare PWA.

As informações geradas pelo cookie não serão compartilhadas com terceiros.

Você pode recusar o uso de cookies selecionando as configurações apropriadas em seu navegador. No entanto, observe que talvez você não consiga usar todos os recursos neste caso. Para obter mais informações, visite:
https://matomo.org/privacy-policy/ .

A base legal para o processamento de dados pessoais dos usuários é o Art. 6 par. 1 frase 1 lit. um GDPR. O tratamento dos dados pessoais dos utilizadores permite-nos analisar o comportamento de utilização. Ao avaliar os dados obtidos, podemos compilar informações sobre o uso dos componentes individuais dos nossos serviços. Isso nos ajuda a melhorar continuamente nossos serviços e sua usabilidade.

Processamos e armazenamos dados pessoais apenas pelo tempo necessário para cumprir a finalidade pretendida.

17. TRANSFERÊNCIA SEGURA DE DADOS PESSOAIS

Usamos medidas de segurança técnicas e organizacionais apropriadas para proteger de forma otimizada seus dados pessoais armazenados por nós contra manipulação, perda, destruição ou acesso acidental ou intencional por pessoas não autorizadas. Os níveis de segurança são continuamente revisados em cooperação com especialistas em segurança e adaptados aos novos padrões de segurança.

A troca de dados de e para o aplicativo é criptografada. Usamos TLS e SSL como protocolos de criptografia para transmissão segura de dados. A troca de dados também é criptografada e realizada com pseudochaves.

18. TRANSFERÊNCIAS DE DADOS / DIVULGAÇÃO A TERCEIROS

Só transmitiremos seus dados pessoais a terceiros no âmbito das disposições legais ou com base no seu consentimento. Em todos os outros casos, as informações não serão divulgadas a terceiros, a menos que sejamos obrigados a fazê-lo devido a regulamentos legais obrigatórios (divulgação a órgãos externos, incluindo autoridades de supervisão ou aplicação da lei).

Qualquer transmissão de dados pessoais é criptografada em trânsito.

19. INFORMAÇÕES GERAIS SOBRE CONSENTIMENTO PARA PROCESSAMENTO DE DADOS

Seu consentimento também constitui consentimento para o processamento de dados de acordo com a lei de proteção de dados. Antes de dar o seu consentimento, iremos informá-lo sobre a finalidade do tratamento de dados e o seu direito de oposição.

Se o consentimento também estiver relacionado ao processamento de categorias especiais de dados pessoais, o aplicativo myoncare informará expressamente sobre isso como parte do procedimento de consentimento.

O processamento de categorias especiais de dados pessoais de acordo com o Art. 9 (1) O GDPR só pode ocorrer se isso for exigido por lei e não houver razão para acreditar que seus interesses legítimos impeçam o processamento desses dados pessoais ou que você tenha dado seu consentimento para o processamento desses dados pessoais de acordo com o Art. 9 (2) GDPR.
Para o processamento de dados para o qual seu consentimento é necessário (conforme explicado neste Política de Privacidade), o consentimento será obtido como parte do processo de registro. Após o registro bem-sucedido, os consentimentos podem ser gerenciados nas configurações da conta do Aplicativo Myoncare.
A revogação do seu consentimento só é efetiva para o futuro. O tratamento efetuado até ao momento da revogação permanece lícito (Art. 7 par. 3 GDPR).

20. DESTINATÁRIOS DE DADOS / CATEGORIAS DE DESTINATÁRIOS

Em nossa organização, garantimos que apenas os indivíduos estejam autorizados a processar dados pessoais necessários para cumprir suas obrigações contratuais e legais. Seus dados pessoais e dados de saúde que você insere em nosso **Aplicativo Myoncare** serão disponibilizados para o seu **Prestador de serviços de saúde** e/ou **empresa** diretamente ou por meio de um **Provedor de dados** (dependendo do tipo de uso do **Ferramentas myoncare**).

Em certos casos, os prestadores de serviços apoiam nossos departamentos especializados no cumprimento de suas tarefas. Os acordos de proteção de dados necessários foram concluídos com todos os provedores de serviços que são processadores de dados pessoais. Esses provedores de serviços são Google (Google Firebase), provedores de armazenamento em nuvem e provedores de serviços de suporte.

O Google Firebase é um "banco de dados NoSQL" que permite a sincronização entre o **Portal myoncare do seu provedor de serviços** e o **Aplicativo Myoncare** . O NoSQL define um mecanismo para armazenar dados que não são apenas modelados em relacionamentos tabulares, permitindo um dimensionamento "horizontal" mais fácil em comparação com sistemas de gerenciamento de banco de dados tabular/relacional em um cluster de máquinas.
Para isso, uma pseudo-chave do **aplicativo myoncare é armazenado no Google Firebase** juntamente com o correspondente **plano de medicação**. A transferência de dados é pseudonimizada para a ONCARE e seus prestadores de serviços, o que significa que a ONCARE e seus prestadores de serviços não podem estabelecer um relacionamento com você como titular dos dados. Isso é conseguido criptografando os dados durante transferência entre você e seu **fornecedor de serviços** ou **empresa** (diretamente ou para um **provedor de dados**) e usando pseudo-chaves em vez de identificadores pessoais, como nome ou endereço de e-mail, para rastrear essas transferências. A reidentificação ocorre assim que os dados pessoais chegam à conta do seu **fornecedor de serviços** ou empresa no **Portal myoncare** ou sua conta no **Aplicativo Myoncare**, depois de ter sido verificado por tokens especiais.

Nossos provedores de armazenamento em nuvem oferecem armazenamento em nuvem, que armazena o gerenciador do Firebase que gerencia os URLs do Firebase para o **Portal myoncare**. Além disso, esses provedores de serviços fornecem o domínio de servidor isolado do **Portal myoncare**, onde seus dados pessoais são armazenados. Ele também hospeda os serviços de gerenciamento de arquivos e vídeo do myoncare, que permitem videoconferência criptografada entre você e seu **fornecedor de serviços**, bem como compartilhamento de arquivos. Acesso aos seus dados pessoais por você e seu **fornecedor de serviços** é garantido pelo envio de tokens específicos. Esses dados pessoais são criptografados em trânsito e em repouso e pseudonimizados para a ONCARE e seus prestadores de serviços. Os prestadores de serviços da ONCARE não têm acesso a esses dados pessoais em nenhum momento.

Além disso, usamos provedores de serviços para processar solicitações de serviço (provedores de serviços de suporte) relacionadas ao uso da conta, por exemplo, se você esqueceu sua senha, deseja alterar seu endereço de e-mail salvo, etc. Os acordos de processamento de pedidos necessários foram concluídos com esses provedores de serviços; Além disso, os funcionários encarregados de processar solicitações de serviço foram treinados adequadamente. Após o recebimento de sua solicitação de serviço, você receberá um número de ticket.
Se esta for uma solicitação de serviço relacionada ao uso da sua conta, as informações relevantes que você nos forneceu ao entrar em contato conosco serão encaminhadas a um dos funcionários autorizados do serviço externo. Ele então entrará em contato com você.
Caso contrário, eles continuarão a ser processados por funcionários especialmente aprovados da ONCARE, conforme descrito em "PROCESSAMENTO DE DADOS OPERACIONAIS".

Por meio de nossos provedores de serviços de suporte, usamos a ferramenta RepairCode, também conhecida como Digital Twin Code, uma plataforma de experiência do cliente para lidar com feedback externo com a capacidade de criar tíquetes de suporte. Aqui você pode encontrar a política de privacidade:
https://app.repaircode.de/?main=main-client – Legal/privacidade.
Por fim, mostramos conteúdo do Instagram (provedor: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlanda) (por exemplo, imagens, vídeos ou publicações). Ao clicar em uma postagem vinculada do Instagram, você será redirecionado para o Instagram. O Instagram pode definir cookies e processar dados do usuário.

Quando você visita uma página com postagens vinculadas do Instagram, seu navegador pode se conectar automaticamente aos servidores do Instagram. Isso fornece ao Instagram as informações de que você visitou nosso site, mesmo que não tenha uma conta no Instagram ou não esteja logado. Se você estiver logado, o Instagram pode atribuir a visita à sua conta de usuário.

Política de privacidade: https://privacycenter.instagram.com/policy

21. TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

Para fornecer nossos serviços, podemos usar provedores de serviços localizados fora da União Europeia. Se os dados forem transferidos para um país terceiro onde a proteção de dados pessoais não tenha sido considerada adequada, garantiremos que sejam tomadas medidas apropriadas de acordo com a legislação nacional e europeia e, se necessário, que cláusulas contratuais padrão apropriadas tenham sido acordadas entre as partes do processamento.
Os dados pessoais coletados por este **Aplicativo Myoncare** não é armazenado nas lojas de aplicativos. Uma transferência de dados pessoais para países terceiros (fora da União Europeia ou do Espaço Econômico Europeu) só ocorre se isso for necessário para o cumprimento da obrigação contratual, for exigido por lei ou se você nos tiver dado seu consentimento.

A sincronização do **Aplicativo Myoncare** e o **Portal myoncare** é feito através do Google Firebase. O servidor do Google Firebase está hospedado na União Europeia. No entanto, conforme descrito nos Termos de Serviço do Google Firebase, transferências de dados de curto prazo podem ser feitas para países onde o Google ou seus provedores de serviços estão localizados; Para determinados serviços do Google Firebase, os dados são transferidos apenas para os Estados Unidos, a menos que o processamento ocorra na União Europeia ou no Espaço Econômico Europeu. O acesso ilegal aos seus dados é impedido com criptografia de ponta a ponta e tokens de acesso seguro. Nossos servidores estão hospedados na Alemanha e para clientes dos EUA nos EUA. Para fins de análise, os e-mails enviados com o SendGrid contêm o chamado "pixel de rastreamento" que se conecta aos servidores do Sendgrid quando o e-mail é aberto. Isso pode ser usado para determinar se uma mensagem de email foi aberta.

Incorporamos conteúdo do Instagram fornecido pela Meta Platforms Ireland Ltd. Se você clicar em uma publicação vinculada do Instagram, os dados pessoais (por exemplo, endereço IP, informações do navegador, interações) poderão ser transmitidos para a Meta Platforms Inc. nos EUA ou em outros países terceiros.
A Meta é certificada pela UE-EUA. Data Privacy Framework (DPF), que reconhece um nível adequado de proteção de dados para transferências para os EUA. No entanto, os dados também podem ser transferidos para países para os quais não existe uma decisão de adequação por parte da Comissão Europeia. Nesses casos, podem ser necessárias medidas de proteção adicionais, mas sua eficácia nem sempre pode ser garantida.

Base jurídica
O processamento de dados é baseado no seu consentimento (Art. 6 par. 1 lit. a RGPD). Você pode revogar este consentimento a qualquer momento. A legalidade das operações de processamento de dados que já ocorreram permanece inalterada pela revogação.

Observe que seus dados geralmente serão transmitidos por nós para um servidor SendGrid nos EUA e armazenados lá. Concluímos um contrato com a Sendgrid que contém as Cláusulas Contratuais Padrão da UE. Isto garante que existe um nível de proteção comparável ao da UE. Além disso, medidas técnicas adicionais de proteção foram implementadas, como criptografia de ponta a ponta e restrição estrita de acesso por meio de tokens baseados em função. Isso serve para proteger ainda mais a transferência de dados no sentido da decisão "Schrems II" do TJUE.

Para processar dados de atividade, interfaces para os serviços do Google Cloud (no caso do GoogleFit) ou para AppleHealth ou Withings são usadas no dispositivo móvel do usuário do aplicativo. **Ferramentas myoncare** use essas interfaces, fornecidas pelo Google, Apple e Withings, para solicitar dados de atividade de aplicativos de saúde conectados. A solicitação enviada por **Ferramentas myoncare** não contém nenhum dado pessoal. Os dados pessoais são disponibilizados para **Ferramentas myoncare** por meio dessas interfaces.

22. DURAÇÃO DO ARMAZENAMENTO DE DADOS PESSOAIS

Manteremos seus dados pessoais pelo tempo necessário para a finalidade para a qual são processados. Observe que vários períodos de retenção exigem o armazenamento contínuo de dados pessoais. Isso se aplica em particular, mas não exclusivamente, às obrigações de retenção sob o direito comercial ou tributário (por exemplo, Código Comercial, Lei Tributária, etc.). Além disso, seu **prestador de serviço de saúde** também deve garantir a retenção de seus registros médicos (entre 1 e 30 anos, dependendo do tipo de documentos).

Observe que a ONCARE também está sujeita a obrigações de retenção que são contratualmente acordadas com seu **fornecedor de serviços** com base em disposições legais. Além disso, e somente se o seu **provedor de serviços utiliza** a variante do dispositivo médico das **Ferramentas myoncare**, certos períodos de retenção resultantes da Lei de Dispositivos Médicos se aplicam devido à classificação do **Aplicativo Myoncare** como um dispositivo médico. Os dados pessoais são normalmente apagados assim que não forem mais necessários, a menos que seja necessária a sua retenção.

Além disso, podemos reter dados pessoais se você nos der seu consentimento para fazê-lo ou se surgir uma disputa e usarmos evidências dentro dos prazos de prescrição legais, que podem ser de até 30 anos. O prazo de prescrição regular é de três anos.

23. OBRIGAÇÃO DE FORNECER DADOS PESSOAIS

Vários dados pessoais são necessários para o estabelecimento, execução e rescisão da relação contratual e o cumprimento das obrigações contratuais e legais associadas. O mesmo se aplica ao uso de nossos Aplicativo Myoncare e as várias funções que oferece.

Resumimos os detalhes para você nos pontos mencionados acima. Em certos casos, os dados pessoais também devem ser coletados ou disponibilizados de acordo com a lei. Observe que, sem o fornecimento desses dados pessoais, não é possível processar sua solicitação ou cumprir a obrigação contratual subjacente.

24. DIREITOS DE ACESSO

Para todos os dispositivos, independentemente do sistema operacional utilizado, é necessário conceder ao aplicativo certas permissões, que chamamos de "direitos básicos de acesso". Dependendo do sistema operacional do dispositivo que você está usando, ele pode ter recursos adicionais que exigem permissões adicionais para que o aplicativo funcione. Para que o **Aplicativo Myoncare** funcione em seu dispositivo, o aplicativo deve receber várias permissões para acessar determinados recursos do dispositivo. Se necessário, iremos listá-los em ordem de sistema operacional (Android ou iOS) de acordo com o "Framework".
Os direitos básicos de acesso (Android e iOS) são:

Obter conexões Wi-Fi
Necessário para garantir a funcionalidade de download de documentos em conjunto com conexões Wi-Fi.

Obter conexão de rede
Necessário para garantir a funcionalidade de download de documentos em conjunto com conexões de rede que não sejam conexões Wi-Fi.

Desative o bloqueio de tela (evite o modo de espera)

Necessário para que os vídeos que pertencem aos documentos fornecidos possam ser reproduzidos diretamente no aplicativo sem serem interrompidos por um bloqueio de tela.

Acesso a todas as redes
O acesso a todas as redes é necessário para baixar documentos.

Desativando o modo de suspensão
Isso é necessário para que os vídeos que pertencem aos documentos fornecidos possam ser reproduzidos diretamente no aplicativo sem que a reprodução seja interrompida pela ocorrência de hibernação.

Dados móveis / Acesso a dados móveis
Caso o usuário queira baixar documentos exclusivamente via Wi-Fi, ele pode fazer a configuração apropriada no menu do app e desativar o uso de dados móveis. O acesso aos dados móveis é necessário para garantir a funcionalidade de desabilitar downloads de documentos em dados móveis.

Acessando a câmera
O acesso à câmera é necessário para leitura de código QR e consultas de vídeo

Acessando o microfone
O acesso ao microfone é necessário para consultas por vídeo

Acesso a arquivos e fotos
Isso é necessário para a troca de arquivos entre você e os usuários do portal conectados.

Acesso ao navegador da Web
Isto é necessário para visualizar os arquivos recebidos dos usuários do portal conectado.

Usamos notificações push, que são mensagens enviadas para o seu dispositivo móvel como um serviço do **Aplicativo Myoncare** por meio de serviços como o Apple Push Notification Service ou o Google Cloud Messaging Service. Esses serviços são recursos-padrão de dispositivos móveis. A Política de Privacidade do Provedor de Serviços rege o acesso, uso e divulgação de informações pessoais como resultado do uso desses serviços.

25. DECISÕES AUTOMATIZADAS CASO A CASO

Não usamos processamento puramente automatizado para tomar decisões.

26. SEUS DIREITOS COMO TITULAR DOS DADOS

Gostaríamos de informá-lo sobre seus direitos como titular dos dados. Esses direitos estão estabelecidos nos artigos 15 a 22 do GDPR e incluem:

Direito de acesso (Art. 15 RGPD): Você tem o direito de solicitar informações sobre se e como seus dados pessoais estão sendo processados, incluindo informações sobre as finalidades do processamento, destinatários, período de armazenamento e seus direitos de retificação, exclusão e objeção. Você também tem o direito de receber uma cópia de quaisquer dados pessoais que mantemos sobre você.

Direito ao apagamento / direito ao esquecimento (Art. 17 RGPD): Você pode solicitar que excluamos seus dados pessoais coletados e processados por nós sem atrasos indevidos. Nesse caso, solicitaremos que você exclua o **Aplicativo Myoncare** incluindo seu UID (Número de Identificação Único) do seu smartphone/celular. Observe, no entanto, que só podemos excluir seus dados pessoais após o término dos períodos de retenção legais.
Direito de retificação (Art. 16 GDPR): Você pode nos pedir para atualizar ou corrigir dados pessoais imprecisos ou para completar dados pessoais incompletos.
Direito à portabilidade de dados (Art. 20 GDPR): Em princípio, você pode solicitar que forneçamos dados pessoais que você nos forneceu e que são processados automaticamente com base em seu consentimento ou na execução de um contrato com você em formato legível por máquina para que possam ser "transferidos" para um provedor de serviços substituto.

Direito à limitação do tratamento de dados (Art. 18 RGPD): Você tem o direito de solicitar a restrição do processamento de seus dados pessoais se a exatidão dos dados for contestada, o processamento for ilegal, os dados forem necessários para fazer valer reivindicações legais ou se uma objeção ao processamento estiver sendo examinada.

Direito de se opor ao processamento de dados (Art. 21 RGPD): Você tem o direito de se opor ao uso de seus dados pessoais e de retirar seu consentimento a qualquer momento quando estivermos processando seus dados pessoais com base em seu consentimento. Continuaremos a fornecer nossos serviços mesmo que eles não dependam da retirada do consentimento. Uma revogação só é eficaz para o futuro. O tratamento efetuado até ao momento da revogação mantém-se lícito.

Para exercer esses direitos, entre em contato primeiro com seu **fornecedor de serviços** ou **empresa** ou entre em contato conosco em: privacy@myoncare.com . A objeção e a revogação do consentimento devem ser declaradas em forma de texto para privacy@myoncare.com .

Exigimos que você forneça provas suficientes de sua identidade para garantir que seus direitos sejam protegidos e que seus dados pessoais sejam compartilhados apenas com você e não com terceiros.

Entre em contato conosco a qualquer momento em privacy@myoncare.com se você tiver alguma dúvida sobre o processamento de dados em nossa empresa ou se quiser retirar seu consentimento. Você também tem o direito de entrar em contato com a autoridade supervisora de proteção de dados competente.

27. OFICIAL DE PROTEÇÃO DE DADOS

Você pode entrar em contato com nosso responsável pela proteção de dados para todas as perguntas sobre proteção de dados em

privacy@myoncare.com.

28. RESTRIÇÃO DE IDADE DO APLICATIVO

É necessária uma idade mínima de 18 anos para usar o **Aplicativo Myoncare** .

29. ALTERAÇÕES À POLÍTICA DE PRIVACIDADE

Reservamo-nos expressamente o direito de alterar isso **Política de privacidade** no futuro, a nosso exclusivo critério. Podem ser necessárias alterações ou aditamentos, por exemplo, para cumprir requisitos legais, para ter em conta a evolução técnica e económica ou **fazer justiça** aos interesses do aplicativo **ou** usuários do portal.
As alterações são possíveis a qualquer momento e serão comunicadas a você de maneira apropriada e em um prazo razoável antes de entrarem em vigor (por exemplo, publicando uma Política de Privacidade revisada no login ou notificando com antecedência as alterações materiais).

Em caso de questões de interpretação ou disputas, apenas a versão alemã da política de privacidade é vinculativa e autoritária.

ONCARE GmbH Endereço postal: Balanstraße 71a, 81541 Munique, Alemanha

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

Dados de contato do Encarregado da Proteção de Dados: privacy@myoncare.com

Para transações na loja myoncare – especialmente em conexão com planos de tratamento (pathways) – a responsabilidade econômica e relacionada ao conteúdo é da myon.clinic GmbH, uma subsidiária da Oncare GmbH. Neste contexto, a Oncare GmbH fornece apenas a plataforma técnica.

Última atualização em junho de 2025.

* * *

A seguir estão os regulamentos suplementares de proteção de dados para usuários nos Estados Unidos da América:

A HIPAA protege as informações de saúde de identificação pessoal (PHI) somente se forem processadas no contexto dos EUA. sistema de saúde por uma entidade compatível com HIPAA – ou seja, uma entidade coberta ou parceiro comercial – independentemente da cidadania ou residência do titular dos dados.

US Política de Privacidade Suplementar para Usuários nos Estados Unidos da América (HIPAA)

Escopo:
Esta seção complementa a Política de Privacidade para usuários residentes nos Estados Unidos da América (EUA) ou para casos em que Protegido Informações de saúde (PHI) é processado de acordo com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA).

Aplica-se em todos os estados dos EUA, na medida em que a ONCARE ou parceiros comissionados processam dados de saúde como um *Parceiro de negócios* em nome de *Entidades cobertas* (por exemplo, médicos ou clínicas) no contexto de processos de tratamento.

1. Base jurídica nos EUA

O processamento de informações pessoais de saúde nos EUA é regido pela **Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (HIPAA)** e alterações subsequentes, incluindo, mas não se limitando a:

- HIPAA **Regra de privacidade** (45 CFR Parte 160 e Subpartes A e E da Parte 164)
- HIPAA **Regra de segurança** (Subpartes A e C da Parte 164)
- **Regra de notificação de violação da HIPAA** (Subparte D da Parte 164)
- e, além disso, a Lei HITECH de 2009

Esses regulamentos se aplicam independentemente do estado dos EUA em que o paciente ou a agência de processamento esteja.

2. O papel da ONCARE como parceiro de negócios

A ONCARE GmbH e as empresas afiliadas nos EUA atuam exclusivamente como **Sócios** no sentido da HIPAA quando **prestar serviços relacionados com o processamento de PHI em nome de prestadores de cuidados de saúde *(*entidades cobertas**). Um Acordo de Parceiro Comercial (BAA) de acordo com 45 CFR §164.504 (e) rege as obrigações de proteção de dados para essas entidades. Neste âmbito, a ONCARE compromete-se:

- Fornecimento da plataforma myoncare (vídeo, comunicação, monitoramento)
- Processamento de Dados Técnicos e Hospedagem
- Fornecimento de funções de suporte algorítmico (por exemplo, triagem)

A ONCARE não fornece **Serviços médicos** e **não toma decisões médicas** no sentido de diagnóstico, terapia ou prescrição.

3. Tipo de dados processados (PHI)

Para os fins da HIPAA, PHI é definida como qualquer informação que:

- Estejam relacionadas com o estado de saúde ou o tratamento de um doente identificável, e
- em conexão com uma *Entidade Coberta* ou seu parceiro de negócios.

As PHI processadas pela ONCARE incluem, em particular:

- Histórico médico (sintomas, fatores de risco)
- Dados de monitoramento (sinais vitais, dados wearable)
- Interações do usuário em questionários estruturados ou ferramentas de triagem
- Histórias de comunicação com profissionais de saúde

4. Direitos dos pacientes sob a HIPAA

Todos os usuários afetados nos EUA tem o direito de:

- **Informação** sobre as PHI armazenadas sobre ele (45 CFR §164.524)
- **Correção** de PHI incorreta ou incompleta (45 CFR §164.526)
- **Limitação** de Divulgação ou Uso em Certos Casos (45 CFR §164.522)
- **Comunicação confidencial** a pedido do paciente
- **Objeção** a certas divulgações (na medida permitida por lei)
- **Contabilidade** de Divulgações (45 CFR §164.528)
- **Reclamação** para os EUA Departamento de Saúde e Serviços Humanos (Escritório de Direitos Civis)

A ONCARE fornece interfaces técnicas para implementar esses direitos mediante solicitação.

Para fazer valer esses direitos, você pode fazer uma solicitação informal por meio do aplicativo myoncare ou entrar em contato conosco por e-mail. A implementação geralmente ocorre dentro de 30 dias, de acordo com 45 CFR §164.524 et seq. Se o pedido for complexo, o prazo pode ser prorrogado uma vez por mais 30 dias. A ONCARE fornece formatos de exportação digital e interfaces de acesso para esse fim.

5. Medidas de segurança de acordo com a regra de segurança

A ONCARE está comprometida em cumprir todos os requisitos da Regra de Segurança HIPAA, incluindo:

Medidas administrativas

- Conceitos internos de proteção e acesso a dados
- Orientações escritas sobre a regulamentação do acesso
- Análises de risco e auditorias regulares
- Treinamento de funcionários com foco na HIPAA

Além disso, a ONCARE está comprometida em realizar regularmente uma "Avaliação de Risco de Segurança" estruturada de acordo com 45 CFR §164.308 (a) (1) (ii) (A) para identificar, avaliar e tomar as medidas apropriadas sobre os riscos de segurança.

Medidas técnicas

- Criptografia de todas as PHI em repouso e em trânsito
- Controle de acesso baseado em função
- Registro em log e histórico de acesso
- Autenticação de dois fatores para equipe médica

Medidas físicas

- Localizações de servidor seguras com controle de acesso
- Conceitos de recuperação de desastres
- Restrições de acesso a hardware e endpoint

6. Proteção de dados na triagem automatizada

A plataforma myoncare contém uma função de triagem estruturada que avalia as informações do paciente (por exemplo, sintomas) com base em critérios definidos e cria **uma avaliação técnica dos riscos**.

Este recurso:

- **não substitui um diagnóstico médico**,
- **não decide de forma independente sobre tratamento ou intervenção**,
- **informa apenas os prestadores de serviços autorizados** (entidades cobertas) de informações potencialmente relevantes.

A ONCARE não se responsabiliza clinicamente por decisões tomadas por médicos ou clínicas com base nessas informações.

7. Divulgação de PHI e outros usos

A ONCARE compartilha PHI apenas com:

- aos prestadores de cuidados de saúde elegíveis no contexto dos cuidados,
- às autoridades de supervisão, se exigido por lei,
- incidentes de segurança sob o **Regra de notificação de violação** (dentro de 60 dias do conhecimento de acordo com 45 CFR §164.404),
- nunca para fins de publicidade, distribuição ou uso de terceiros sem o consentimento expresso e documentado do paciente.

Qualquer divulgação ou uso de PHI para fins de pesquisa, marketing ou outros fins de terceiros só ocorrerá após autorização prévia documentada de acordo com 45 CFR §164.508. Sem esse consentimento expresso, tal divulgação não ocorrerá.

Uso de dados não identificados para fins comerciais
A ONCARE pode usar dados de saúde e uso que foram desidentificados de acordo com a Regra de Privacidade da HIPAA (45 CFR §164.514) para análise interna, melhoria da plataforma, desenvolvimento de novos serviços de saúde e outros fins comerciais.

Depois que os dados são desidentificados, eles não são mais considerados Informações de Saúde Protegidas (PHI) e não estão sujeitos às proteções da Regra de Privacidade da HIPAA.

8. Contacto para o exercício de direitos

Responsável por questões relacionadas à HIPAA:
ONCARE GmbH
Balanstraße 71a80339 MuniqueAlemanhaE-mail: privacy@myoncare.com

EUA Os cidadãos também podem entrar em contato com o **EUA Departamento de Saúde e Serviços Humanos - Escritório de Direitos Civis (OCR)** diretamente com reclamações: https://www.hhs.gov/ocr/

9. Integração de fornecedores terceirizados, dados de lojas virtuais e isenção de responsabilidade

9.1 Envolvimento de fornecedores técnicos terceirizados (fabricantes de dispositivos, distribuidores de dispositivos médicos e laboratórios)

No âmbito da plataforma myoncare e sua subsidiária myon.clinic, **fornecedores terceirizados, como fabricantes de dispositivos, distribuidores de dispositivos médicos ou laboratórios médicos** pode ser conectado ao sistema, se necessário. Isso é feito exclusivamente para apoiar o cuidado medicamente responsável e é baseado nas instruções do respectivo *Entidades cobertas*.

Os provedores de serviços terceirizados conectados processam informações de saúde de identificação pessoal (PHI) somente sob acordo contratual e em conformidade com os requisitos da HIPAA. Você também está sujeito aos requisitos de proteção de dados do 45 CFR §164.502(e) como um *subcontratado* de um parceiro de negócios e estão vinculados por **Acordos de subcontratação (sub-BAA**).

9.2 Coleta de dados no contexto de ofertas de lojas virtuais

Ao adquirir programas de saúde digital, os chamados programas de saúde digital. **Pathways**ou produtos afiliados através da loja virtual da subsidiária **myon.clinic**, os dados pessoais, incluindo PHI, podem ser processados para fins de processamento e manutenção desses programas. Isto aplica-se, em especial:

- Dados de uso da funcionalidade Pathway,
- sintomas especificados ou dados de diagnóstico,
- quaisquer códigos de saúde resgatados ou informações sobre o produto.

A coleta é realizada em conformidade com as Regras de Privacidade e Segurança da HIPAA e exclusivamente para uma finalidade específica. A divulgação a fornecedores terceirizados só ocorrerá com base em um sub-BAA existente ou com consentimento documentado.

Qualquer divulgação de PHI (Informações de Saúde Protegidas) fora da cadeia contratual (por exemplo, para pesquisa ou marketing) requer um documento **"autorização"** de acordo com 45 CFR §164.508.

9.3 Isenção de responsabilidade para avaliação médica e efeitos colaterais

A ONCARE GmbH e suas empresas afiliadas não assumem **qualquer avaliação médica ou obrigação de notificar reações adversas a medicamentos, efeitos colaterais do produto ou outros riscos relacionados à saúde.**

Responsabilidade legal por:

- o diagnóstico e a selecção de uma via ou de um produto,
- a avaliação dos riscos ou contra-indicações,
- bem como os legalmente exigidos **notificação de efeitos secundários** ou eventos de segurança para autoridades reguladoras ou fabricantes

cabe exclusivamente ao médico assistente ou à oferta **Entidade coberta** ou o dispositivo responsável ou fabricante do medicamento.

A plataforma **fornece apenas a infraestrutura técnica** e não assume qualquer responsabilidade médica ou regulatória pelo conteúdo, resultados ou consequências de qualquer aplicação por pacientes ou prestadores de serviços.

Regra de Preempção e Conformidade com a Lei Estadual

A Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) fornece um **Nível mínimo de proteção de dados de acordo com a lei federal** que se aplica em todos os EUA. estados. Ao mesmo tempo, 45 CFR §160.203 permite o chamado **preempção**, ou seja, regulamentações mais rígidas de estados individuais podem substituir a HIPAA em certos aspectos se:

- assegurar uma maior proteção dos titulares dos dados, ou
- requisitos especiais para dados de saúde ou dados de saúde eletrônicos.
- A ONCARE e suas afiliadas estão expressamente comprometidas em cumprir todas as leis federais relevantes, incluindo, mas não se limitando a:

- **Lei de Privacidade do Consumidor da Califórnia (CCPA/CPRA)**
- **Lei de Privacidade Médica do Texas (TMPA)**

- **Lei SHIELD de Nova York**
- **Regulamentos de segurança de dados de Massachusetts**
- bem como leis de proteção de dados comparáveis em nível estadual

Na medida em que a ONCARE atua em nome das Entidades Cobertas, o processamento é realizado em conformidade com os padrões de proteção de dados estaduais aplicáveis e com a HIPAA, desde que sejam mais rigorosos do que os requisitos da HIPAA. Em caso de desvios, a regulamentação que **oferece ao paciente em causa um nível mais elevado de proteção de dados** sempre se aplica.

Além dos regulamentos nacionais da HIPAA, leis adicionais de proteção de dados se aplicam em estados individuais, como Califórnia, Nova York ou Texas. Na medida em que essas leis têm requisitos mais rígidos do que a HIPAA, elas têm precedência. Nestes casos, a ONCARE cumprirá a legislação aplicável mais rigorosa.

11. Exercício dos direitos da HIPAA (procedimentos, verificação de identidade, prazos)

Usuários residentes nos EUA ou cujos dados são processados pela U.S. as entidades cobertas têm os direitos estabelecidos na Seção 4 desta Política de Privacidade de acordo com a HIPAA.

Os seguintes regulamentos se aplicam ao exercício desses direitos:

11.1 Aplicação

Os direitos da HIPAA podem ser exercidos por:

- Pedido por escrito por correio eletrónico para: **privacy@myoncare.com**
- Solicitação por escrito sobre o respectivo prestador de serviços de saúde (*Entidade coberta*)

11.2 Verificação de identidade

Para a proteção do titular dos dados, qualquer pedido de exercício de direitos só será processado após **verificação bem-sucedida da identidade**. As medidas possíveis incluem:

- Comparação com dados utilizados durante o registo
- Apresentação de um documento de identidade válido com foto (em upload seguro)
- Confirmação do médico assistente

11.3 Prazos de processamento

O ONCARE processa solicitações:

- **dentro de 30 dias corridos** a contar da data de recepção do pedido,
- Extensão para **mais 30 dias** é permitido uma vez; O requerente é informado por escrito e recebe a justificação
- todas as perguntas e respostas serão documentadas e arquivadas de acordo com 45 CFR §164.530 (j).

12. Processamento de dados fora dos Estados Unidos (offshoring / localização de dados)

Em certos casos, o processamento de PHI pode ser realizado em nome de um US. Entidade coberta **fora dos Estados Unidos**, nomeadamente:

- pela ONCARE GmbH, com sede na Alemanha (UE),
- para fornecer serviços de infraestrutura técnica, hospedagem, suporte e desenvolvimento de produtos.

Este tratamento transfronteiriço é realizado exclusivamente:

- com base em um **Acordo de Parceiro Comercial** (BAA),
- com documentação explícita no Plano de Gerenciamento de Riscos HIPAA da Entidade Coberta,
- com conformidade com a Regra de Segurança HIPAA, bem como **medidas de segurança de acordo com o padrão europeu GDPR**, nomeadamente:

- → Criptografia de ponta a ponta (AES-256),
- → Restrição de acesso de acordo com o princípio da necessidade de saber,
- → Registro de todos os acessos com trilha de auditoria,
- → Armazenamento de dados apenas em servidores com controle de acesso físico e certificação ISO 27001.

PHI é **não armazenado em sistemas fora dos EUA sem medidas técnicas de proteção apropriadas** e proteção contratual.

Medidas administrativas

A ONCARE implementou medidas administrativas sob 45 CFR §164.308 para todos os serviços relacionados aos EUA, incluindo:

- **Diretores de proteção de dados e diretores de nível empresarial da HIPAA**
- **Políticas de privacidade e segurança**, com controle de versão, documentado e apoiado por treinamento
- **Treinamento obrigatório para todos os funcionários** que trabalham com dados de saúde dos EUA (pelo menos anualmente)
- **Regras de sanções** por violações de proteção de dados, conforme definido pelo 45 CFR §164.530 (e)
- **Avaliação do sistema baseada em risco e avaliações de vulnerabilidade**, pelo menos uma vez por ano ou em caso de alterações significativas do sistema

Todos os processos são documentados em um **Manual de conformidade com HIPAA**, que é regularmente atualizado e revisto na auditoria interna.

14. Salvaguardas técnicas da regra de segurança HIPAA

A ONCARE implementou totalmente medidas técnicas de proteção de acordo com 45 CFR §164.312:

Categoria	Medida
Controle de acesso	Acesso baseado em função, IDs de usuário exclusivos, logout automático de sessão, procedimentos de acesso de emergência
Controles de auditoria	Sistema completo e registro de acesso com avaliação regular
Controles de integridade	Verificações de integridade baseadas em hash e controle de versão para dados médicos críticos
Autenticação	Autenticação de dois fatores para equipe médica e administradores
Segurança de transmissão	Criptografia TLS 1.3 durante a transmissão, proteção VPN para todos os provedores de serviços externos

Essas medidas se aplicam a todos os sistemas que armazenam, processam ou transmitem PHI. A implementação é assegurada anualmente por testes técnicos de penetração e um **Análise de risco em conformidade com a HIPAA** .

***