

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

Bem-vindo ao myoncare, o portal de saúde digital para atendimento eficiente e baseado nas necessidades do paciente.

Para nós da Oncare GmbH (doravante denominada "**ONCARE**" ou "**nós**", "**Nós**", "**nosso**"), a proteção de sua privacidade e de todos os dados pessoais relacionados a você durante o uso do Portal myoncare é de grande importância. Estamos cientes da responsabilidade que decorre do fornecimento e armazenamento de seus dados pessoais no portal myoncare (= plataforma). 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.

Esta Política de Privacidade consiste em duas partes:

- A primeira parte contém regulamentos de proteção de dados para o uso da plataforma myoncare na Europa com base no Regulamento Geral de Proteção de Dados (GDPR).
- A segunda parte contém disposições suplementares de acordo com os requisitos da Lei de Proteção de Dados dos EUA (HIPAA). Estes aplicam-se em particular **se os dados de saúde forem processados por uma entidade coberta pelos EUA ou se os prestadores de serviços operarem dentro da estrutura do sistema de saúde dos EUA** – independentemente da residência da pessoa em causa.

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 descobrirá por que e como **ONCARE** Processa seus dados pessoais que coletamos de você ou que você nos fornece quando decide usar o Portal myoncare. Em particular, você encontrará uma descrição do tipo de dados pessoais que coletamos e processamos, bem como a finalidade e a base sobre a qual processamos os dados pessoais; Além disso, você encontrará os direitos aos quais tem direito aqui.

Leia atentamente a Política de Privacidade para a compreensão de cada item aqui disposto. Após ler a Política de Privacidade, você terá a oportunidade de consentir com a Política de Privacidade e consentir com o processamento de seus dados pessoais conforme descrito na Política de Privacidade. Se você der seu consentimento, a Política de Privacidade passa a fazer parte do contrato entre você e a **ONCARE**.

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

1. DEFINIÇÕES

"Usuário do aplicativo" significa qualquer usuário do Aplicativo myoncare (seu paciente).

"Tecnologia Blockchain" O sistema myoncare contém um banco de dados adicional no qual os dados de todas as instalações são armazenados.

"Provedor de Careplan" significa você ou qualquer outro prestador de serviços ou terceiro (por exemplo, fabricante de dispositivos médicos, empresa farmacêutica) que disponibiliza Planos de Assistência a outros usuários do Portal através da Loja myonclinic ou outros meios de troca de dados.

"Usuário do Careplan" significa você ou outro prestador de serviços (Usuário do Portal) que utiliza um Care Plan ("Pathway") para o tratamento de seus Pacientes Cadastrados.

"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 prestadores de cuidados envolvidos, pela equipe de enfermagem ou pelo próprio paciente.

"Provedor" significa você ou qualquer outro médico, clínica, estabelecimento de saúde ou outro profissional de saúde agindo sozinho ou em seu nome ou em nome de você ou de outro médico, clínica ou estabelecimento de saúde (Usuário Pretendido).

"Aplicativo myoncare" significa o aplicativo móvel myoncare para pacientes que desejam usar os serviços oferecidos pela **ONCARE** por meio do Aplicativo.

"Loja myonclinic" é a plataforma operada pela **ONCARE** que fornece conceitos de cuidados digitais (planos de tratamento) para o tratamento de seus pacientes cadastrados por meio do portal myoncare.

"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** por meio do PWA e não por meio do aplicativo myoncare.

"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.

"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 você ou outro prestador de serviços que usa o Portal myoncare baseado na web.

"Política de Privacidade do Paciente" significa a Política de Privacidade que descreve a coleta, o uso e o armazenamento das informações pessoais (de saúde) dos Pacientes que usam o Aplicativo myoncare. 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.

"Política de privacidade" significa esta declaração fornecida a você como usuário do Portal myoncare, que descreve como coletamos, usamos e armazenamos seus dados pessoais e informa sobre seus amplos direitos.

"Termos de Uso" significa os termos e condições de uso para o uso do Portal 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 e opera o portal interativo da web Portal myoncare (para profissionais de saúde) e o aplicativo móvel Aplicativo myoncare (para os doentes) como acesso aos Serviços myoncare. Esta **política de privacidade** se aplica a todos os dados pessoais processados pela **ONCARE** em conexão com o uso do **Portal myoncare**. Para o uso do **Aplicativo Myoncare** por pacientes, você pode encontrar separadamente a Política de Privacidade para Pacientes Aqui: <https://www.myoncare.com/privacy-policy>

3. O QUE SÃO DADOS PESSOAIS

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

"Dados pessoais" significa qualquer informação que permita identificar uma pessoa singular. Isso inclui, mas não se limita a, 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, **"pseudonimizado"** Dados são dados a partir dos quais uma referência pessoal ou informação de identificação pessoal é substituída por um ou mais identificadores artificiais ou pseudônimos, mas que geralmente podem ser reidentificados pela chave identificadora. (na acepção do Art. 4 No. 5 GDPR).

Myoncare PWA

Um aplicativo da web progressivo (PWA) é um site que parece e tem a funcionalidade de um aplicativo móvel. Os PWAs são projetados 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 seção.

4. 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 **Portal myoncare**, entrando em contato conosco sobre problemas com o portal ou interagindo conosco com a finalidade de usar o portal.

Dados de tratamento: Você coleta dados pessoais de seus pacientes, como nome, idade, altura, peso, indicação, sintomas de doença e outras informações relacionadas ao tratamento de seus pacientes (por exemplo, em um care plan) no **Portal myoncare**. Os dados de atividade de seus pacientes conectados são disponibilizados para você em seu **Portal myoncare**.

Dados da loja comercial: Dados da Loja Comercial: Dados pessoais processados em conexão com o uso da Loja myonclinic – 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 da atividade: Dados pessoais processados por nós quando um **O usuário do aplicativo se conecta o Aplicativo Myoncare** para um aplicativo de saúde (por exemplo, AppleHealth, GoogleFit, Withings). Os dados de atividade de seus pacientes conectados são disponibilizados para você em seu **Portal myoncare**.

Análise de dados de uso anônimos para melhoria da plataforma:

Processamos apenas dados técnicos de uso anônimos e não pessoais (por exemplo, informações agregadas sobre frequência de uso ou desempenho do sistema) para desenvolver ainda mais a funcionalidade e a experiência do usuário do portal. Esses dados não contêm informações de identificação e não permitem tirar conclusões sobre usuários individuais do portal. Os dados pessoais dos prestadores de serviços de saúde não são processados para fins de pesquisa ou comerciais.

Dados de fabricantes de dispositivos ou laboratórios:

Além disso, os dados pessoais podem ser processados por fabricantes de dispositivos médicos conectados ou prestadores de serviços laboratoriais como parte de processos de atendimento integrado, 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 no caso de você relatar um incidente, a fim de garantir a segurança jurídica ou a vigilância de empresas de dispositivos médicos ou farmacêuticas.

Dados de reembolso: Dados pessoais necessários para o processo de reembolso.

5. TECNOLOGIA BLOCKCHAIN

Blockchain **Tecnologia ("Blockchain")** (Patente Europeia n.º 4 002 787) é um serviço **opcional** que não é obrigatório. Cabe a você, o **fornecedor de serviços**, para decidir 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 há um banco de dados adicional no qual os dados do aplicativo são armazenados. 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.

O **blockchain** geralmente 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

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

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. Nesse caso, o bloco não pode mais ser sincronizado com os demais. 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. Se todos os nós (nós de rede) tentarem sincronizar suas cópias, será determinado que a cópia modificada foi modificada e a rede considerará esse nó não íntegro. Este processo técnico impede que pessoas não autorizadas manipulem o conteúdo da cadeia blockchain.

Nosso **blockchain** é um **blockchain privado**. 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", **Blockchains privados** são "autorizados" porque a autorização é necessária para se tornar um usuário. Ao contrário do público **Blockchains**, acessíveis ao público a todos, o acesso a **Blockchains privados** depende de autorização para se tornar um usuário. Essa estrutura permite alavancar a segurança e a imutabilidade de **Tecnologia Blockchain** mantendo-se em conformidade com a proteção de dados, em particular em conformidade 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 Universal Exclusivo) no 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 de apagar "direito de ser esquecido", Art. 17 do RGPD).

Tipo de dados armazenados e processados em blockchain:

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

Os dados armazenados no **blockchain** é pseudonimizado.

Nosso **blockchain** foi projetado para garantir a privacidade dos dados em termos de integridade, perfil do paciente, ativos e atribuídos **care tasks** e medicamentos. Para se comunicar com o **Cadeia de blocos**, o usuário deve registrar um conjunto de chaves públicas e privadas. Para se comunicar com o **blockchain**, o usuário precisa de várias chaves públicas e privadas; O processo de registro gera certificados que são armazenados em um banco de dados separado do **prestador de serviços de saúde** e no celular do paciente. Uma cópia de backup da chave do paciente é armazenada de forma criptografada no **banco de dados do 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 concordou com o **provedor**. O **blockchain** assim, serve para garantir a integridade e responsabilidade do protocolo 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 concordar com a política de privacidade, essa interação será armazenada no **blockchain**. Toda vez que há uma comunicação com o paciente, o blockchain responde comparando o hash a um marcador indicando 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 está fora de sincronia ou não 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.

Justificativa do tratamento: O tratamento de dados pela ONCARE em nome da **fornecedor de serviços** é realizado com base no Art. 28 GDPR (contrato de processamento de dados).

6. PROCESSAMENTO DE DADOS OPERACIONAIS

Caso você seja uma pessoa de contato para a operação do Portal em seu local/consultório (por exemplo, administrador de TI, profissional médico nomeado), você pode nos fornecer determinados dados pessoais quando entrar em contato conosco para entender ou discutir as funções e o uso do Portal, ou no caso de uma solicitação de serviço.

No caso de uma solicitação de serviço, os seguintes dados pessoais também podem ser visualizados por funcionários autorizados da ONCARE: Seus dados pessoais que você nos forneceu para registro e/ou login em nosso portal (por exemplo, nome, data de nascimento, foto de perfil, detalhes de contato). Os funcionários autorizados da ONCARE que estão autorizados a acessar seu banco de dados para fins de processamento de uma solicitação de serviço são contratualmente obrigados a manter todos os dados pessoais estritamente confidenciais.

Explicações importantes sobre 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:

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

- Enviamos notificações push por meio de nosso **myoncare PWA** (Progressive Web App) e o **Aplicativo Myoncare** para informá-lo sobre tarefas, prazos 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 garantirá que você não perca nenhuma notificação importante e que seu suporte funcione sem problemas.

Por que fazemos isso:

Nosso objetivo é garantir que você esteja sempre informado sobre suas tarefas e atualizações importantes, a fim de apoiar de forma otimizada seus cuidados.

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.

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

Tipos de dados: endereço de e-mail, data de nascimento, data de registro, seu endereço IP, pseudo-chaves geradas pelo portal.

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 **Portal myoncare** e para entrar em contato com você se necessário ou diretamente iniciado por você (por exemplo, em caso de alterações nos termos e condições, suporte necessário, problemas técnicos, etc.). Além disso, os dados pessoais (endereço de e-mail) são processados no âmbito da autenticação de dois fatores sempre que inicia sessão no **Portal myoncare**.

Justificativa do tratamento: O processamento de dados operacionais 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 **portal myoncare**.

7. 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 Geoapify (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 reter-los. Para obter mais informações sobre suas políticas de privacidade, consulte <https://ipapi.com/privacy/> e [Política de Privacidade | Plataforma de localização geoapify](#).

8. PROCESSAMENTO DE DADOS DE (TRATAMENTO)

Ao usar o **Portal myoncare**, você insere dados pessoais (relacionados à saúde) de seus pacientes no **Portal myoncare** (por exemplo, fornecimento de um plano de tratamento individual, lembrete para tomar medicamentos, etc.). Além disso, você e seus pacientes podem fazer upload de documentos e arquivos para o **Portal myoncare** e compartilhá-los uns com os outros. Além disso, as funções de localização podem ser geradas e implementadas:

- Adicionando um local;
- Upload do logotipo do site;
- Adicionando os detalhes do local;
- Carregar uma política de privacidade;

É possível criar outros requisitos de consentimento para o paciente, para os quais o paciente deve fornecer consentimento para se conectar ao site. Uma política de privacidade carregada será exibida para todos os pacientes que se conectarem ao site. Todas as declarações de consentimento devem ser documentadas na política de privacidade carregada. Depois que uma política de privacidade é carregada, ela só pode ser substituída por uma nova versão, mas não pode ser excluída.

Os arquivos são armazenados em um banco de dados em nuvem na Alemanha. Você pode permitir o compartilhamento de tais arquivos com outros **Usuários do portal** dentro de sua instituição para fins médicos. Outros **Usuários do portal** não têm acesso a esses arquivos.

Pode também consultar um prestador de serviços externo à sua instituição (médico consultor) no contexto do tratamento dos seus doentes, se considerar que outro perito serve o tratamento.

De acordo com o GDPR, como controlador de dados, você é responsável pelo processamento de dados de saúde dos pacientes no contexto do uso dos serviços myoncare.

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

Processamos esses dados pessoais, incluindo os dados de saúde do paciente, sob um contrato com você e de acordo com suas instruções. Processe os dados de seus pacientes apenas se você tiver obtido o consentimento de dados necessário desses pacientes. A ONCARE atua como processadora de acordo com o contrato de processamento de dados separado que celebramos com você com base no Art. 28 GDPR.

9. PROCESSAMENTO DE USO TÉCNICO E DADOS DO SISTEMA

Aplica-se apenas se você usar a Loja myonclinic como usuário do Careplan.

O **Loja myonclinic** está integrado ao **Portal myoncare** e oferece a compra de planos de tratamento (Careplan). Depois de se registrar no **Portal myoncare**, você pode se conectar ao **Loja myonclinic** com seus dados de login. Você pode usar o **Loja myonclinic** para adquirir planos de tratamento como usuário.

Dados do usuário do Careplan:

Os dados do **Usuário do Careplan**, que a **Loja myonclinic** processa durante o uso, é processado com a finalidade de celebrar um contrato de licença com o **Provedor de Careplan** – neste caso, a ONCARE – e, se for devida uma taxa, pelo processamento e controle do processo de pagamento entre os **Provedores de Careplan** – neste caso, a ONCARE – e o **Usuário do Careplan**.

Tipos de dados: nome, dados de contato, dados bancários.

Tratamento de dados de lojas comerciais: Dados pessoais processados por nós ao usar a **Loja myonclinic** como parte da compra de planos de tratamento. Além disso, os dados de pagamento (se for cobrada uma taxa de utilização) serão **encaminhado ao provedor do Careplan**.

Justificação do tratamento de dados de lojas comerciais: A base legal para o processamento de dados de lojas comerciais é o Art. 6 (1) (b) GDPR – o processamento dos dados serve para a execução do contrato entre o **usuário do Careplan** e o **provedor do Careplan** – neste caso, a ONCARE.

10. PROCESSAMENTO DE DADOS DE ATIVIDADE

Aplicável somente se os usuários do aplicativo conectados consentirem e habilitarem a transferência de dados.

Ferramentas myoncare oferecem **Usuários do aplicativo** a opção de conectar o **Aplicativo Myoncare** para certos aplicativos de saúde (por exemplo, AppleHealth, GoogleFit, Withings) ("**Aplicativo Saúde**"), desde que sejam utilizados pelo **Usuário do aplicativo** e a conexão é estabelecida pelo **Usuário do aplicativo**. Uma vez conectado, os dados de atividade coletados pelos **Aplicativo de Saúde** serão disponibilizados a você para fornecer informações contextuais adicionais sobre o **Usuário do aplicativo**. Observe que os dados da atividade não se originam de **Ferramentas myoncare** e, portanto, não deve ser usado para fins de diagnóstico como base para decisões médicas.

O processamento de dados de atividade é de responsabilidade de seus pacientes.

Tipos de dados: O tipo e o escopo dos dados transferidos dependem da decisão do **Usuários do aplicativo**. Os dados incluem peso, altura, passos dados, calorias queimadas, horas de sono, frequência cardíaca e pressão arterial, entre outros.

Finalidade do processamento de dados de atividade: O **Usuário do aplicativo de Dados de Atividade** é fornecido a você para fornecer informações contextuais adicionais sobre a **atividade do Usuário do aplicativo**. Observe que os dados da atividade não são validados pelas **ferramentas myoncare** e não deve ser usado para fins de diagnóstico ou como base para decisões médicas.

Motivo do processamento:

O controlador de dados é o próprio paciente, dando-lhe acesso aos dados de sua atividade para verificar as informações compartilhadas. Por conseguinte, não há necessidade de mais justificações.

11. PROCESSAMENTO DE DADOS DE SEGURANÇA DO PRODUTO

Aplica-se apenas se você usar a variante de dispositivo médico das ferramentas myoncare.

O **Portal myoncare** e o **Aplicativo Myoncare** são classificados e comercializados como dispositivos médicos de acordo com os regulamentos europeus de dispositivos médicos. Como fabricante das **ferramentas myoncare**, temos que cumprir certas obrigações legais (por exemplo, monitorar a funcionalidade da ferramenta, avaliar relatórios de incidentes que possam estar relacionados ao uso da ferramenta, rastrear usuários, etc.). Além disso **as ferramentas myoncare** permitem que você colete dados pessoais sobre dispositivos médicos ou medicamentos específicos usados no tratamento de seus pacientes. 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: relatórios de casos, dados pessoais fornecidos em um relatório de incidente e resultados da avaliação, detalhes do relator.

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 obrigações de supervisão. Além disso, armazenamos e transferimos dados pessoais relacionados a dispositivos médicos e/ou medicamentos quando recebemos comunicações suas como relator de tais informações, de seu paciente ou de terceiros (por exemplo, nossos distribuidores ou importadores de **ferramentas myoncare** em seu país) que devem ser relatados ao fabricante do produto para que ele cumpra suas obrigações legais sobre segurança do produto.

Justificativa para o processamento de dados de segurança do produto:

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

A base legal para o processamento de dados pessoais para o cumprimento de obrigações legais como fabricante de dispositivos médicos ou medicamentos 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 respectivos fabricantes dos produtos utilizados.

12. PROCESSAMENTO POR FABRICANTES DE EQUIPAMENTOS E PRESTADORES DE SERVIÇOS DE LABORATÓRIO

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 terceiros externos (por exemplo, fabricantes de dispositivos médicos 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.

13. 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.

12. PROCESSAMENTO DE DADOS DE REEMBOLSO EM CASO DE TRANSMISSÃO DE OBJETO DE CUSTO

(Aplicável apenas se você usar as ferramentas myoncare para reembolso.)

O **Portal myoncare** apoia-o no início dos seus procedimentos normalizados para o reembolso dos serviços de saúde que prestou aos seus doentes através do **Aplicativo Myoncare**. Para habilitar o processo de reembolso, o **Portal myoncare** suporta a coleta de dados pessoais (relacionados à saúde) de seus pacientes a partir do **Portal myoncare** a fim de facilitar a transmissão desses dados aos pagadores do paciente como parte dos processos de reembolso padrão (sua Associação de Médicos de Seguro de Saúde Estatutário e/ou a companhia de seguro de saúde do paciente). Você é o controlador de dados para os dados de reembolso e é responsável por cumprir os regulamentos de proteção de dados para o processamento dos dados pessoais de seus pacientes no processo de reembolso. A ONCARE atua como Processador de Dados com base no Contrato de Processamento de Dados com o **Fornecedor de serviços**.

Tipos de dados: nome do paciente, diagnóstico, indicações, tratamento, duração do tratamento, outros dados necessários para o gerenciamento do reembolso.

Tratamento dos dados relativos ao reembolso: Você, como controlador, transmite os dados de tratamento do paciente necessários para reembolso ao pagador (sua companhia de seguros de saúde e/ou a companhia de seguros de saúde do paciente) e o pagador processa os dados de reembolso para reembolsá-lo.

Motivo do processamento de dados de reembolso: O processamento de dados de reembolso é realizado com base no §§ 295, 301 SGB V. O processamento de dados pela ONCARE para você também é realizado com base no Art. 28 GDPR (contrato de processamento de pedidos).

13. QUAL TECNOLOGIA É USADA PELO PORTAL MYONCARE E PELO APLICATIVO MYONCARE?

O **Portal myoncare** funciona como uma ferramenta baseada na web para a qual você precisa de uma conexão de internet funcional e uma versão atualizada do navegador de internet Chrome, Firefox ou Safari.

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;

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

- Elaboração e envio de relatório;
- Substitua as notificações push por e-mails para **PWA** (Progressive Web App) nos seguintes casos:
 - Se um care plan terminar dentro de um dia;
 - 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.

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.

Brevo (Política de Privacidade):

[Política de Privacidade - Proteção de Dados Pessoais | Brevo](#)

SendGrid

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

- Sistema operacional do usuário;
- Geolocalização do usuário;
- Navegador;
- Função;
- Endereço IP;
- Sites visitados via Web/PWA (consulte a seção sobre PWA nesta Política de Privacidade para obter mais informações);
- Botões nos quais o usuário clica no arquivo **Portal myoncare**, no **Aplicativo Myoncare** e no **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, por favor 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 dos utilizadores. 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.

14. 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 portal, bem como de e para o aplicativo, é criptografada. Oferecemos SSL como um protocolo de criptografia para transmissão segura de dados. A troca de dados também é criptografada e realizada com pseudochaves.

15. TRANSFERÊNCIA DE DADOS OU DIVULGAÇÃO A TERCEIROS

Seus dados pessoais só serão repassados 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.

As informações sobre como lidamos com os dados pessoais (de saúde) de seus pacientes que usam o **Aplicativo Myoncare** é resumido em um **política de privacidade** pelo **Aplicativo do paciente myoncare**. Você pode encontrar a **Política de Privacidade para Pacientes** [aqui](#). Por favor, leia também esta Política de Privacidade do Paciente cuidadosamente. Você é o controlador de dados para parte do processamento de dados do paciente e é responsável pela conformidade com a proteção de dados (por exemplo, transmissão de dados de tratamento para o paciente).

16. 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 **Portal myoncare** irá informá-lo expressamente sobre isso como parte do procedimento de consentimento.

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

Processamento de categorias especiais de dados pessoais de acordo com o Art. 9 (1) O GDPR só pode ocorrer se isso for necessário devido a disposições legais e não houver razão para supor 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 **Portal myoncare**. Além disso, a ONCARE solicitará que você concorde com um contrato de processamento de dados para os dados processados pela ONCARE sob sua responsabilidade como controlador.

17. DESTINATÁRIOS DE DADOS OU CATEGORIAS DE DESTINATÁRIOS

Em nossa organização, garantimos que apenas as pessoas que são obrigadas a fazê-lo para cumprir suas obrigações contratuais e legais têm o direito de processar dados pessoais.

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 **Portal myoncare** e o **Aplicativo Myoncare** é armazenado no Google Firebase junto com o plano de tratamento correspondente. 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 em trânsito e usando pseudo-chaves em vez de identificadores pessoais, como nomes ou endereços de e-mail, para rastrear essas transferências. A reidentificação ocorre assim que os dados pessoais chegam à conta do paciente no **Aplicativo Myoncare** ou sua conta no **Portal myoncare** após verificação por tokens específicos.

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 são armazenados os seus dados pessoais e os dos seus pacientes. Ele também hospeda o serviço de gerenciamento de vídeo e arquivos do myoncare, que permite videoconferência criptografada e compartilhamento de dados entre você e seu paciente. O acesso aos seus dados pessoais por si e pelo seu paciente é assegurado através do envio de tokens específicos. Esses dados pessoais são criptografados durante a transmissão e pseudonimizados para a ONCARE e seus prestadores de serviços durante a transmissão e em repouso. 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. Esta é uma plataforma de experiência do cliente para lidar com feedback externo com a capacidade de para criar tíquetes de suporte. Aqui você encontrará o 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>

18. 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.

Dados pessoais coletados pelo **Portal myoncare** ou o **Aplicativo Myoncare** não são 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 **Portal myoncare** com o **Aplicativo Myoncare** é feito com a ajuda do Google Firebase. Os servidores do Google Firebase estão hospedados na União Europeia. No entanto, de acordo com os termos e condições gerais do Google Firebase, uma transferência temporária de dados para países nos quais o Google e provedores de serviços relacionados mantêm filiais. 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 não autorizado aos seus dados é impedido por criptografia de ponta a ponta e tokens de acesso seguro. Nossos servidores online estão

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE

A PARTIR DE JUNHO DE 2025

hospedados na Alemanha. 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.

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.

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.

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. As **Ferramentas myoncare** usam essas interfaces, fornecidas pelo Google, Apple e Withings, para solicitar dados de atividade dos aplicativos de saúde conectados. O pedido enviado pelas **ferramentas myoncare** não contém nenhum dado pessoal. Os dados pessoais são disponibilizados para **Ferramentas myoncare** por meio dessas interfaces.

19. 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 às obrigações de retenção sob o direito comercial ou tributário.

Observe que a ONCARE também está sujeita a obrigações de retenção que são contratualmente acordadas com você com base em disposições legais. Além disso, devido à classificação e, se aplicável, ao uso do **Portal myoncare** e o **Aplicativo Myoncare** como um dispositivo médico, certos períodos de retenção se aplicam ao portal, que resultam da Lei de Dispositivos Médicos. 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.

20. SEUS DIREITOS COMO TITULAR DOS DADOS

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 **Portal myoncare** e as várias funções que oferece.

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.

21. DECISÕES AUTOMATIZADAS EM CASOS INDIVIDUAIS

Não usamos processamento puramente automatizado para tomar decisões.

22. 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, bem como 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 **Portal myoncare** do seu computador. 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 sobre você 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.

Para exercer esses direitos, entre em contato conosco em: privacy@myoncare.com. A objeção e a revogação do consentimento devem ser submetidas a privacy@myoncare.com em forma de texto.

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.

**PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE
A PARTIR DE JUNHO DE 2025**

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.

23. ENCARREGADO 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.

24. SUJEITO A ALTERAÇÕES A ESTA 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 notificadas a você de maneira apropriada e dentro de um prazo razoável antes de sua data de vigência (por exemplo, publicando um relatório revisado **Política de privacidade** no login ou fornecendo aviso prévio de alterações materiais).

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

Se o conteúdo ou serviços médicos forem obtidos ou oferecidos por meio da loja integrada myonclinic, o conteúdo e a responsabilidade econômica serão de responsabilidade da myon.clinic GmbH, uma subsidiária da Oncare GmbH. Neste contexto, a Oncare GmbH fornece apenas a plataforma técnica. privacy@myon.clinic

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

A PARTIR DE JUNHO DE 2025

O seguinte **são regulamentos suplementares de proteção de dados para provedores de serviços** que atuam como uma entidade coberta nos Estados Unidos da América **como parte de** uma atividade em conformidade com a HIPAA **ou em nome de tal entidade**:

A proteção de informações pessoais de saúde (PHI) sob a HIPAA só se aplica se esses dados forem processados dentro da estrutura dos EUA. sistema de saúde por uma entidade chamada coberta ou um parceiro comercial – independentemente da nacionalidade ou residência do titular dos dados. O único fator decisivo é que o processamento se enquadre no escopo da HIPAA.

US Regulamentos Suplementares de Proteção de Dados para Provedores de Serviços nos Estados Unidos da América (HIPAA)

1. Escopo de aplicação

Este Adendo da HIPAA se aplica a todos os provedores de serviços que processam, armazenam ou compartilham informações de saúde protegidas (PHI) por meio da plataforma ONCARE, desde que tal processamento esteja em conexão com um contratado regulamentado pela HIPAA ("Entidade Coberta") ou a ONCARE atue como parceira comercial.

2. Funções e responsabilidades

A ONCARE está atuando como parceira comercial de acordo com a Regra de Privacidade da HIPAA (45 CFR §160.103) e está comprometida em cumprir todos os regulamentos HIPAA aplicáveis à Entidade Coberta. O respectivo prestador de serviços atua:

- como membro da força de trabalho da entidade coberta ou
- como subcontratado da ONCARE de acordo com 45 CFR §160.103 et seq.

3. Quadro de processamento

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

O uso da plataforma ONCARE por provedores de serviços é baseado apenas em acordos existentes em conformidade com a HIPAA com a entidade coberta (por exemplo, acordos de parceiros comerciais ou contratos de provedores de serviços). O processamento inclui, em particular:

- Documentação de cursos de tratamento e serviços médicos,
- Comunicação com pacientes usando canais de comunicação compatíveis com HIPAA (criptografia de ponta a ponta, TLS)
- Acesso a dados estruturados do paciente para atendimento ou garantia de qualidade.

4. Confidencialidade e controle de acesso

Os provedores concordam em manter todas as PHI confidenciais e limitar o acesso às PHI na medida do necessário, de acordo com o Padrão Mínimo Necessário (45 CFR §164.502 (b)). Cada acesso é gerenciado por meio de um conceito de direitos baseado em função e registrado de maneira auditável.

5. Medidas de segurança técnicas e organizacionais

Todas as medidas de segurança implementadas pela ONCARE estão em conformidade com os requisitos da Regra de Segurança HIPAA (45 CFR Parte 164, Subparte C). Esses incluem:

- Criptografia AES-256 de dados armazenados,
- transmissão criptografada via TLS 1.3,
- Autenticação de dois fatores (2FA),
- análises periódicas de risco de acordo com §164.308 (a) (1) (ii) (A),
- processos estruturados de resposta a incidentes.

6. Processamento de dados fora dos EUA

Quando os Provedores acessam dados por meio do ONCARE que são processados ou armazenados fora dos Estados Unidos (por exemplo, hospedagem na UE), eles o fazem exclusivamente:

- com base na proteção contratual compatível com HIPAA (por exemplo, BAA de subcontratado),
- com consentimento documentado da Entidade Coberta,
- em conformidade com a Regra de Segurança HIPAA e normas internacionais complementares (por exemplo, B. ISO 27001, princípios GDPR),
- e com criptografia e controle de acesso de ponta a ponta.

7. Obrigações de comunicação em caso de incidentes de proteção de dados

Os provedores são obrigados a notificar imediatamente a ONCARE sobre qualquer incidente que possa levar ao acesso não autorizado a PHI ("Incidente de Segurança" ou "Violação", conforme definido em 45 CFR §164.304/§164.402). A ONCARE assume a coordenação dos relatórios legalmente exigidos para a entidade coberta e as pessoas afetadas.

8. Direitos da Entidade Coberta

A Entidade Coberta reserva-se o direito de, a qualquer momento, auditar o acesso, o uso e as medidas de segurança relativas às PHI pela ONCARE e pelos Prestadores de Serviços Associados. Os prestadores de serviços devem garantir total cooperação.

9. Sem distribuição independente

O Provedor de Serviços só pode divulgar PHI a terceiros fora da Plataforma (por exemplo, por e-mail, sistema externo, impressão) se:

- existe uma "autorização" documentada pelo titular dos dados ou
- Isso está expressamente previsto no contrato.

10. Precedência e interpretação

Em caso de conflito entre este Suplemento da HIPAA e as regras europeias de proteção de dados, a regra mais rígida sempre será aplicada, desde que seja consistente com a lei aplicável. EUA as leis federais de privacidade (por exemplo, CCPA) permanecem e as leis estaduais de privacidade, não são afetadas e se aplicam adicionalmente, quando aplicável.

11. Apoio aos direitos dos titulares dos dados

Os prestadores de serviços apoiam a ONCARE e a respectiva Entidade Coberta no cumprimento dos direitos dos titulares dos dados de acordo com 45 CFR §§ 164.524–528 (por exemplo, informações, correção, restrição de divulgação). Tal inclui, nomeadamente, a participação em:

- o fornecimento de registros de acesso ("Contabilidade de Divulgações"),
- a correção de PHI errônea,
- a implementação de avisos de bloqueio ou restrições de uso.

As solicitações serão coordenadas pela ONCARE e processadas com aviso prévio de 30 dias, com possível prorrogação de mais 30 dias após a notificação.

12. Obrigação de ministrar formação em matéria de proteção de dados

Os provedores de serviços são obrigados a realizar um curso de treinamento documentado sobre os requisitos de proteção de dados de acordo com HIPAA e GDPR todos os anos.

A ONCARE fornece materiais adequados ou acesso a e-learning para esse fim. A participação é documentada digitalmente e deve ser comprovada à Entidade Coberta mediante solicitação.

13. Dados de uso secundário e pesquisa

PLATAFORMA MYONCARE – PROVEDOR DE SERVIÇOS DE POLÍTICA DE PRIVACIDADE A PARTIR DE JUNHO DE 2025

Qualquer uso de PHI para fins de pesquisa, análise ou marketing pelo Provedor de Serviços é proibido, a menos que:

- há um consentimento documentado ("Autorização") de acordo com 45 CFR §164.508,
 - ou um contrato específico de uso de dados de pesquisa compatível com HIPAA foi concluído com a ONCARE.
- O uso secundário interno (por exemplo, para garantia de qualidade) só é permitido dentro do escopo da limitação de finalidade da HIPAA.

14. Coordenação com os requisitos do GDPR

Com a aplicabilidade simultânea do GDPR e da HIPAA, a ONCARE garante que o nível mais rigoroso de proteção sempre se aplique. Em particular, os prestadores de serviços comprometem-se a:

- não transferir dados para fora do EEE sem as Cláusulas Contratuais Padrão ou sub-BAA's apropriados;
- Coordenar os direitos do titular dos dados de ambas as jurisdições (por exemplo, direito de exclusão nos termos do Art. 17 GDPR vs. obrigações de retenção de acordo com a HIPAA) de acordo com a ONCARE.

15. Requisitos suplementares de proteção de dados estaduais (EUA)

Além dos regulamentos federais sob a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), certos processamentos de dados estão sujeitos a leis de proteção de dados suplementares ou mais rígidas de estados individuais dos EUA. Isso se aplica em particular se os usuários afetados residirem em um desses estados, usarem nossos serviços de lá ou se os dados pessoais forem processados por provedores de serviços ou parceiros contratuais baseados nesses estados.

As seguintes leis federais de privacidade podem ser aplicadas adicionalmente ou com prioridade, dependendo da constelação individual:

- Califórnia: Lei de Privacidade do Consumidor da Califórnia (CCPA) e Lei de Direitos de Privacidade da Califórnia (CPRA)
- Nova Iorque: Lei SHIELD
- Virgínia: Lei de Proteção de Dados do Consumidor da Virgínia (VCDPA)
- Colorado: Lei de Privacidade do Colorado (CPA)
- Connecticut: Lei de Privacidade de Dados (CTDPA)
- Utah: Lei de Privacidade do Consumidor de Utah (UCPA)
- Illinois: Lei de Privacidade de Informações Biométricas (BIPA)
- Texas: Lei de Privacidade e Segurança de Dados (TDPSA, em vigor em 01.07.2024)
- Flórida: Declaração de Direitos Digitais (FDBR)

Estamos comprometidos em cumprir os regulamentos federais aplicáveis a todas as atividades de processamento e em fornecer aos titulares dos dados informações abrangentes sobre a aplicação desses direitos, mediante solicitação. Para determinados estados (por exemplo, Califórnia), fornecemos avisos de privacidade separados mediante solicitação. Entre em contato conosco em privacy@myoncare.com se você quiser exercer seus direitos relacionados à privacidade de acordo com a lei federal ou estadual.

16. Sem uso comercial dos dados pessoais do usuário do portal

Os dados pessoais dos usuários do portal (por exemplo, prestadores de serviços de saúde) não são usados para pesquisa, marketing ou quaisquer outros fins comerciais. A ONCARE processa apenas dados técnicos de uso totalmente anônimos (por exemplo, carimbos de data/hora de login agregados ou padrões de uso do sistema) para melhorar o desempenho técnico da plataforma. Esses dados não contêm nenhuma informação que possa ser usada para identificar usuários individuais e não são considerados Informações de Saúde Protegidas (PHI) de acordo com a Regra de Privacidade da HIPAA.
