POLITIQUE DE CONFIDENTIALITÉ POUR L'EUROPE

Bienvenue sur myoncare, le portail de santé numérique pour des soins efficaces et adaptés aux besoins.
Pour nous, chez Oncare GmbH (ci-après dénommée «**ONCARE"** ou «**nous**", **"Nous**", "**notre**"), la protection de votre vie privée et de vos données personnelles traitées lors de l'utilisation du portail myoncare est d'une grande importance. Nous sommes conscients de la responsabilité qui découle de la mise à disposition et de l'enregistrement de vos données personnelles sur le portail myoncare. Par conséquent, nos systèmes technologiques utilisés pour les services myoncare sont configurés selon les normes les plus élevées et le traitement légal des données est au cœur de notre compréhension éthique en tant qu'entreprise.

Nous traitons vos données personnelles conformément aux dispositions légales applicables en matière de protection des données personnelles, en particulier le Règlement général sur la protection des données de l'UE («**RGPD »)** et les lois spécifiques à chaque pays qui s'appliquent à nous. Dans cette politique de confidentialité, vous découvrirez pourquoi et comment **ONCARE** Traite vos données personnelles que nous collectons auprès de vous ou que vous nous fournissez lorsque vous décidez d'utiliser le portail myoncare. En particulier, vous trouverez une description du type de données personnelles que nous collectons et traitons, ainsi que la finalité et la base sur lesquelles nous traitons les données personnelles ; En outre, vous y trouverez les droits qui vous sont accordés.

Veuillez lire attentivement la politique de confidentialité pour vous assurer que vous comprenez chaque disposition. Après avoir lu la politique de confidentialité, vous aurez la possibilité de consentir à la politique de confidentialité et de consentir au traitement de vos données personnelles comme décrit dans la politique de confidentialité. Si vous donnez votre consentement, la politique de confidentialité fait partie du contrat entre vous et ONCARE.

En cas de questions d'interprétation ou de litiges, seule la version allemande de la politique de confidentialité est contraignante et fait foi.

DÉFINITIONS

« Utilisateur de l'application» désigne tout utilisateur de l'Application myoncare (votre patient).

"Technologie blockchain" Le système myoncare contient une base de données décentralisée supplémentaire dans laquelle sont stockées les données de toutes les installations.

"Fournisseur de Careplan» désigne vous ou tout autre prestataire de services ou tiers (par exemple, un fabricant de dispositifs médicaux, une société pharmaceutique) qui met des plans de soins à la disposition d'autres utilisateurs du portail via le myoncare Store ou d'autres moyens d'échange de données.

"Utilisateur du Careplan» désigne vous ou tout autre prestataire de services (Utilisateur du Portail) qui utilise un Careplan (« Care Pathway ») pour le traitement de ses Patients enregistrés.

"Pathway" est un plan de traitement standardisé composé de plusieurs tâches de soins programmées, qui peuvent déterminer les étapes des diagnostics et des thérapies. **"CareTasks"** sont tâches spécifiques ou actions au sein d'un pathway qui doivent être réalisées par les prestataires de soins concernés, le personnel soignant ou le patient lui-même.

"**Fournisseur de soins de santé**» désigne vous ou tout autre médecin, clinique, établissement de santé ou autre professionnel de la santé agissant seul ou en votre nom ou au nom d'un autre médecin, d'une clinique ou d'un établissement de santé (l'utilisateur visé).

"**L'application myoncare**» fait référence à l'application mobile myoncare pour les patients qui souhaitent utiliser les services proposés par ONCARE via l'application.

"**Magasin myoncare"** est la plateforme exploitée par **ONCARE** qui fournit des concepts de soins numériques (careplans) pour le traitement de vos patients enregistrés via le portail myoncare.

"**Outils myoncare**» désigne l'application myoncare et le portail myoncare.

"L'application myoncare PWA» désigne l'application myoncare Progressive Web App pour les patients qui souhaitent utiliser les services proposés par ONCARE via l'application PWA et non via l'application myoncare.

"**Portail myoncare**" est le portail web myoncare destiné à un usage professionnel par les utilisateurs du portail et sert d'interface entre les utilisateurs du portail et les patients en tant qu'utilisateurs de l'application.

"**Services myoncare**» désigne les services, fonctionnalités et autres offres qui sont ou pourraient être proposés aux utilisateurs du portail via le portail myoncare et/ou aux utilisateurs de l'application via l'application myoncare.

"**ONCARE**» désigne ONCARE GmbH, Allemagne.

"**Utilisateur du portail**» désigne vous ou tout autre prestataire de services utilisant le portail Web myoncare.

"**Politique de confidentialité des patients**» désigne la politique de confidentialité qui décrit la collecte, l'utilisation et le stockage des informations personnelles (de santé) des patients utilisant l'application myoncare. Selon les conditions d'utilisation, notre offre s'adresse uniquement aux patients âgés de 18 ans et plus. Par conséquent, aucune donnée personnelle d'enfants et d'adolescents de moins de 18 ans n'est stockée et traitée.

"**Politique de confidentialité**» désigne la présente déclaration qui vous est fournie en tant qu'utilisateur du Portail myoncare, qui décrit la manière dont nous recueillons, utilisons et stockons vos informations personnelles et vous informe de vos droits généraux.

"**Conditions d'utilisation**» désigne les conditions d'utilisation pour l'utilisation du Portail myoncare.

TRAITEMENT DES DONNÉES

Oncare GmbH, une société immatriculée au tribunal d'instance de Munich sous le numéro d'enregistrement 219909 dont le siège social est situé Balanstraße 71a, 81541 Munich, Allemagne, propose et exploite le portail web interactif myoncare Portal (pour les professionnels de la santé) et l'application mobile myoncare App (pour les patients) comme accès aux services myoncare. Cette **politique de confidentialité** s'applique à toutes les données personnelles traitées par ONCARE dans le cadre de l'utilisation du portail myoncare. Pour l'utilisation de l'application myoncare par les patients, vous trouverez une politique de confidentialité distincte pour les patients **ici**.

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

"**Données personnelles**» désigne toute information permettant d'identifier une personne physique. Cela inclut, mais sans s'y limiter, votre nom, votre date de naissance, votre adresse, votre numéro de téléphone, votre adresse e-mail et votre adresse IP.

"**Données de santé"** désigne les données personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de services de santé, dont découlent les informations relatives à son état de santé.

Les données doivent être considérées comme «**anonyme**" si aucun lien personnel avec la personne/l'utilisateur ne peut être établi.
En revanche, «**pseudonymisé**Les données sont des données dont une référence personnelle ou une information personnellement identifiable est remplacée par un ou plusieurs identifiants artificiels ou pseudonymes, mais qui peuvent généralement être réidentifiées par la clé d'identification. (au sens de l'art. 4 n° 5 du RGPD).

Application Myoncare PWA

Une application web progressive (PWA) est un site web qui a l'apparence et les fonctionnalités d'une application mobile. Les PWA sont conçues pour tirer parti des fonctionnalités natives des appareils mobiles sans avoir besoin d'un magasin d'applications. L'objectif des PWA est de combiner la différence entre les applications et le Web traditionnel en apportant les avantages des applications mobiles natives dans le navigateur. La PWA est basée sur la technologie de « React ». « React » est un logiciel open-source pour les applications PWA.

Pour utiliser l' **application myoncare PWA**, les patients ont besoin d'un ordinateur ou d'un smartphone et d'une connexion Internet active. Il n'est pas nécessaire de télécharger une application.

Certains des services de l'application myoncare ne peuvent pas être utilisés dans l' **application myoncare PWA**, voir la description ci-dessous pour plus de détails. Il s'agit des services ou spécifications suivants :
-Discuter avec des **prestataires de soins de santé**;
-Vidéo;
- Codes PIN de sécurité;
-Suivi des données d'activité (par exemple via AppleHealth, GoogleFit, Withings).
Les informations suivantes sur l' **application myonCare** s'applique également à l' **application myoncare PWA**, sauf indication contraire dans le présent article.

QUELLES DONNÉES PERSONNELLES SONT UTILISÉES LORS DE L'UTILISATION DE L'APPLICATION MYONCARE

Nous pouvons traiter les catégories de données suivantes vous concernant lors de l'utilisation de l'**application myoncare**:

Données opérationnelles : Données personnelles que vous nous fournissez lors de votre inscription et de votre connexion à notre **portail myoncare**, lorsque vous nous contactez au sujet de problèmes avec le portail ou lorsque vous interagissez avec nous dans le but d'utiliser le portail.

Données de traitement: Vous collectez des données personnelles de vos patients, telles que le nom, l'âge, la taille, le poids, l'indication, les symptômes de la maladie et d'autres informations en rapport avec le traitement de vos patients (par exemple dans le cadre d'un careplan) dans le **portail myoncare**. Les données d'activité de vos patients connectés sont mises à votre disposition dans votre **portail myoncare**.

Données du store commercial: Données personnelles que nous traitons dans le cadre de l'utilisation de **myoncare store**, soit dans le cadre de la paternité de careplans, soit dans le cadre de l'achat de careplans. L'utilisation de **myoncare store** nécessitera le traitement de votre nom et d'autres coordonnées ainsi que des détails de paiement (informations de paiement uniquement si le careplan est payant).

Données d'activité: Données personnelles que nous traitons lorsqu'un **utilisateur de l'application** relie l' **application myoncare** à une application de santé (par exemple AppleHealth, GoogleFit, Withings). Les données d'activité de vos patients connectés sont mises à votre disposition dans votre **portail myoncare**.

Données de recherche commerciales et non commerciales:
Nous traitons vos données personnelles sous forme anonymisée/pseudonymisée pour analyser et produire des rapports scientifiques synthétiques afin d'améliorer les produits, les traitements et les résultats scientifiques.

Données de sécurité du produit: Données personnelles qui sont traitées pour se conformer à nos obligations légales en tant que fabricant de **l'application myoncare** en tant que dispositif médical. En outre, vos informations personnelles peuvent être traitées dans le cas où vous signalez un incident à des fins de sécurité juridique ou de vigilance des entreprises de dispositifs médicaux ou pharmaceutiques.

Données de remboursement: Données personnelles nécessaires au processus de remboursement.

TECHNOLOGIE BLOCKCHAIN

Technologie Blockchain ("**Blockchain**") (Brevet européen n° 4 002 787) est un service facultatif qui n'est pas obligatoire. C'est à vous, **fournisseur de soins de santé**, de décider d'utiliser la solution blockchain. Le **blockchain** est basé sur la technologie d'Hyperledger Fabric. Hyperledger Fabric est un logiciel open source pour les implémentations de blockchain au niveau de l'entreprise. Il offre une plateforme évolutive et sécurisée qui prend en charge les projets de blockchain.

La **blockchain** dans le système myoncare est une base de données supplémentaire qui stocke les données de l'application. Toutes les données de la blockchain sont stockées en République fédérale d'Allemagne. Il s'agit d'une **chaîne de blocs** ("**Blockchain privée**"), elle permet uniquement la saisie de participants vérifiés sélectionnés, et il est possible d'écraser, de modifier ou de supprimer des entrées selon les besoins.

En général, la **blockchain** se compose de données numériques dans une chaîne de paquets appelés «blocs» qui stockent les transactions correspondantes. La façon dont ces blocs sont reliés les uns aux autres est chronologique. Le premier bloc créé est appelé bloc de genèse, et chaque bloc ajouté par la suite a un hachage

cryptographique lié au bloc précédent, ce qui permet de retracer les transactions et les modifications d'informations jusqu'au bloc de genèse. Toutes les transactions à l'intérieur des blocs sont validées et vérifiées par le biais d'un mécanisme de consensus blockchain afin de s'assurer que chaque transaction reste inchangée.

Chaque bloc contient la liste des transactions, un horodatage, son propre hachage et le hachage du bloc précédent. Un hachage est une fonction qui convertit des données numériques en une chaîne alphanumérique. Dans ce cas, le bloc ne peut plus être synchronisé avec les autres. Si une personne non autorisée tente de modifier les données d'un seul bloc, le hachage du bloc changera également et le lien vers ce bloc sera perdu. Si tous les noeuds (noeuds du réseau) tentent de synchroniser leurs copies, il est déterminé que la copie modifiée a été modifiée et le réseau considère que ce noeud est défectueux. Ce processus technique empêche les personnes non autorisées de manipuler le contenu de la chaîne blockchain.

Notre **blockchain** est **blockchain privée**. Une **blockchain** privée est décentralisée. Il s'agit d'un système dit de registre distribué (système numérique d'enregistrement des transactions), qui fonctionne comme une base de données fermée. Contrairement aux **blockchains** publiques, qui sont «non autorisées», les **blockchains** privés sont «autorisées» parce qu'une autorisation est requise pour devenir un utilisateur. Contrairement aux **blockchains** publiques, qui sont accessibles à tous, l'accès aux **blockchains** privées dépend de l'autorisation pour devenir un utilisateur. Cette structure permet de tirer parti de la sécurité et de l'immuabilité de la **technologie blockchain** tout en étant conforme à la protection des données, et de se conformer à la réglementation du Règlement général sur la protection des données (RGPD). Les enregistrements privés de la blockchain peuvent être modifiés, modifiés ou supprimés ; dans ce contexte signifie que la valeur de référence à l'UUID (Universally unique identifier) dans la base de données de **fournisseur de soins de santé** est supprimée. De plus, le hachage est anonymisé dans la base de données blockchain, de sorte que ce processus global est conforme au règlement général sur la protection des données et que les droits d'une personne concernée sont garantis (droit à l'effacement « droit à l'oubli », Art. 17 du RGPD).

Type de données stockées et traitées dans la blockchain:

-Patients-UUID
-Institutions/Leistungserbinger UUID
-Asset-UUID
-Hachage des données de **caretask** et de fichier.
(*UUID : Identifiant Unique Universel*).

Les données stockées dans la **blockchain** est pseudo-anonymisé.
Notre **blockchain** est conçu pour garantir la confidentialité des données en termes d'intégrité des données, de profil du patient, fichiers et d'attribution des **caretasks** et des médicaments. Pour communiquer avec le **blockchain**, l'utilisateur doit enregistrer une série de clés publiques-privées. Pour communiquer avec la **blockchain**, l'utilisateur a besoin de plusieurs clés publiques-privées; le processus d'enregistrement génère des certificats qui sont stockés dans une base de données distincte de **prestataire** de **santé** et sur le téléphone portable du patient. Une copie de sauvegarde de la clé du patient est chiffrée et stockée dans la base de données de **prestataire de santé**, qui n'est accessible qu'au patient.

Lors de la vérification du consentement à la protection des données, dans le cas où le **prestataire de santé** souhaite communiquer avec le patient, le système vérifie si le patient a donné son consentement à la politique de confidentialité du prestataire. La **blockchain** sert donc à assurer l'intégrité et la responsabilité du dossier afin de s'assurer que le patient a accepté la politique de confidentialité.

Lorsqu'un **prestataire de santé** télécharge une nouvelle version d'une politique de confidentialité, le hachage du fichier est stocké dans la **blockchain**, et une fois que le patient a accepté la politique de confidentialité, cette interaction est stockée dans la **blockchain**. Chaque fois qu'elle communique avec le patient, la **blockchain** répond en comparant le hachage avec un indicateur qui indique si le consentement du patient est toujours valide pour la politique de confidentialité actuelle.
L'intégrité du profil du patient est également assurée par la blockchain dans la synchronisation des patients. Le **fournisseur de soins de santé** détecte immédiatement si le profil du patient n'est pas synchronisé ou s'il correspond au profil sur le téléphone mobile en

comparant le hachage du profil du patient dans la **blockchain**. De cette manière, le **fournisseur de soins de santé** obtient une actualité suffisante en ce qui concerne le profil du patient.

Portail myoncare:
Si le **fournisseur de soins de santé** décide d'utiliser la solution blockchain, ONCARE met en œuvre un outil supplémentaire, appelé « Adapter Service », qui sert à communiquer avec la **blockchain**. L'instance blockchain est hébergée par ONCARE.

L'application myoncare:
Les patients peuvent se connecter à la même instance de blockchain à l'aide de l'outil Phone Manager, qui est également hébergé par ONCARE. Ce service est également hébergé par ONCARE.

Justification du traitement: Le traitement des données par ONCARE pour le compte de **fournisseur de soins de santé** est effectué sur la base de l'art. 28 du RGPD (accord de traitement des commandes).

TRAITEMENT DES DONNÉES OPÉRATIONNELLES

Si vous êtes une personne de contact pour l'exploitation du portail sur votre site/cabinet (par exemple, administrateur informatique, professionnel de la santé désigné), vous pouvez nous fournir certaines données personnelles lorsque vous nous contactez pour comprendre ou discuter des fonctionnalités et de l'utilisation du portail, ou en cas de demande de service.

En cas de demande de service, les données personnelles suivantes peuvent également être consultées par les employés autorisés d'ONCARE :

Vos données personnelles que vous nous avez fournies pour l'inscription et/ou la connexion à notre portail (par exemple, nom, date de naissance, photo de profil, coordonnées).

Les employés autorisés d'ONCARE qui peuvent accéder à votre base de données dans le but de traiter une demande de service sont contractuellement tenus de garder tous les renseignements personnels strictement confidentiels.

Explications importantes sur les notifications push et les e-mails
Dans le cadre de votre soutien par myoncare, nous souhaitons vous informer de la manière dont nous traitons les notifications et les informations importantes que nous vous envoyons.

1. **Notifications push**:
    - Nous vous envoyons des notifications push via notre **myoncare PWA** (Progressive Web App) et l' **application myoncare** pour vous informer sur les tâches, les rendez-vous et les mises à jour importantes.
    - Vous avez la possibilité de désactiver ces notifications push dans les paramètres de votre application.
2. **Notifications par e-mail**:
    - Que vous ayez activé ou désactivé les notifications push, nous continuerons à vous envoyer des informations importantes et des rappels par e-mail.
    - Cela vous permet de ne manquer aucune notification importante et de garantir le bon déroulement de votre assistance.

Pourquoi nous faisons cela :

- Notre objectif est que vous soyez toujours informé de vos tâches et des mises à jour importantes pour soutenir de manière optimale vos soins.
- Les e-mails sont un moyen fiable de s'assurer que des informations importantes vous parviennent, même lorsque les notifications push sont désactivées.

Vos options d'action :

- Si vous ne souhaitez pas recevoir de notifications push, vous pouvez les désactiver dans les paramètres de l' **application myoncare**.
- Veuillez vous assurer que votre adresse e-mail est exacte et à jour pour assurer la bonne réception de nos messages.
- Si vous ne souhaitez pas recevoir de rappels par e-mail, vous pouvez les désactiver dans les paramètres de **l'application myoncare**.

Période de conservation
Les données que vous nous fournissez pour recevoir des e-mails seront stockées par nous jusqu'à ce que vous vous déconnectiez de nos services et seront supprimées

de nos serveurs et des serveurs de Sendgrid après votre déconnexion.

Lors du traitement des données opérationnelles, ONCARE agit en tant que contrôleur de données responsable du traitement légal de vos données personnelles.

Types de données: adresse e-mail, date de naissance, date d'inscription, votre adresse IP, pseudo-clés générées par le Portail.

L'application utilise l'API Google Maps pour utiliser les informations géographiques. Pendant l'utilisation de google Maps, Google collecte, traite et utilise également les données relatives à l'utilisation des fonctions de cartes. Vous trouverez des informations plus détaillées sur l'étendue, la base juridique et la finalité du traitement des données par Google ainsi que sur la durée de conservation dans la politique de confidentialité de Google.

Finalité du traitement des données opérationnelles: Nous utilisons les données opérationnelles pour maintenir les fonctionnalités du **portail myoncare** et de vous contacter directement si nécessaire ou à votre initiative (par exemple en cas de modifications des conditions d'utilisation, d'assistance nécessaire, de problèmes techniques, etc.). En outre, les données personnelles (adresse e-mail) sont nécessaires et traitées dans le cadre de l'authentification à deux facteurs chaque fois que vous vous connectez au **portail myoncare**.

Justification du traitement: Le traitement des données opérationnelles est justifié sur la base de l'Art. 6 par. 1 lit. b RGPD pour l'exécution du contrat que vous concluez avec ONCARE dans le but d'utiliser le **portail myoncare**.

GÉOLOCALISATION IP

Nous utilisons une application de géolocalisation pour nos services. Nous utilisons ipapi (fourni par apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Vienne, Autriche) et Geoapify (fourni par Keptago Ltd., N. Nikolaidi et T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Chypre) pour identifier la localisation des patients utilisateurs. Nous les utilisons pour sécuriser nos applications et pour vérifier la localisation de l'utilisateur patient afin de nous assurer que l'utilisation de nos services est conforme. Nous ne combinons pas les informations que nous recueillons avec d'autres informations sur l'utilisateur qui pourraient l'identifier. Les données traitées par apilayer comprennent l'adresse IP du patient et d'autres détails sur la localisation. La base juridique de l'utilisation est l'Art. 6 par. 1 lit. f RGPD. Les données seront supprimées lorsque la finalité associée pour laquelle elles ont été collectées n'existe plus et qu'il n'y a plus d'obligation légale de les stocker. Pour plus d'informations sur leur politique de confidentialité, veuillez consulter https://ipapi.com/privacy/ et Politique de confidentialité | Plateforme de localisation Geoapify.

TRAITEMENT DES DONNÉES CONCERNANT LE TRAITEMENT

En utilisant le **portail myoncare**, vous saisissez les données personnelles (de santé) de vos patients dans le **portail myoncare** (ex : mise à disposition d'un careplan individualisé, rappel de la prise de médicaments, etc.). De plus, vous et vos patients pouvez télécharger des documents et des fichiers dans le **portail myoncare** et les partager les uns avec les autres. De plus, des fonctions de localisation peuvent être générées et implémentées:

- Ajout d'un lieu;
- Mise en ligne du logo du site;
- Ajouter les détails de l'emplacement;
- Télécharger une politique de confidentialité;

Il est possible de créer d'autres exigences de consentement pour le patient, pour lesquelles le patient doit donner son consentement afin de se connecter au site Web.

Une politique de confidentialité téléchargée sera affichée à chaque patient qui se connecte au site Web. Toutes les déclarations de consentement doivent être documentées dans la politique de confidentialité téléchargée. Une fois qu'une politique de confidentialité

a été téléchargée, elle ne peut être remplacée que par une nouvelle version, mais ne peut pas être supprimée. Les fichiers sont stockés dans une base de données cloud en Allemagne. Vous pouvez autoriser le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de votre établissement à des fins médicales. Les autres **utilisateurs du portail** n'ont pas accès à ces fichiers.

De plus, vous pouvez impliquer un **fournisseur de soins de santé** à l'extérieur de votre établissement (prestataire de soins de santé consultant) dans le traitement de vos patients, à condition que vous estimez qu'un avis d'expert supplémentaire serait bénéfique au traitement.

Conformément au RGPD, vous êtes responsable du traitement des données de santé des patients dans le cadre de l'utilisation des services myoncare en tant que responsable des données.

Nous traitons ces données personnelles, y compris les données de santé du patient, dans le cadre d'un accord avec vous et conformément à vos instructions. Veuillez ne traiter les données de vos patients que si vous avez obtenu le consentement requis de ces patients. ONCARE agit en tant que sous-traitant conformément à l'accord de traitement des données séparé que nous avons conclu avec vous sur la base de l'art. 28 du RGPD.

TRAITEMENT DES DONNÉES DES MAGASINS COMMERCIAUX

Applicable uniquement si vous utilisez le myoncare Store en tant qu'utilisateur de Careplan.

Le **myoncare store** est intégré dans le **portail myoncare** et propose l'achat de careplans. Après vous être inscrit sur le **portail myoncare**, vous pouvez vous connecter au **myoncare store** à l'aide de vos données de connexion. Vous pouvez utiliser **myoncare store** pour acheter des careplans en tant qu'utilisateur.

Données de l'utilisateur du careplan:

Les données de l' **utilisateur de careplan**, que **myoncare Store** traite lors de son utilisation, est traité pour la conclusion d'un contrat de licence avec le **prestataire de careplan** – dans ce cas ONCARE – et, si des frais sont dus, pour le traitement et le contrôle de l'opération de paiement entre **le prestataire de careplan** – dans ce cas ONCARE – et **l'utilisateur de careplan**.

Types de données: nom, coordonnées, coordonnées bancaires.

Traitement des données des magasins commerciaux: Données personnelles que nous traitons dans le cadre de l'utilisation de **myoncare store** dans le cadre de l'achat de careplans. En outre, les données de paiement (si des frais d'utilisation sont facturés) seront transmises au **prestataire de careplan**.

Justification du traitement des données des magasins commerciaux: La base juridique du traitement des données des magasins commerciaux est l'Art. 6 par. 1 lit. b RGPD – le traitement des données sert à l'exécution du contrat entre **utilisateur de careplan** et **prestataire de careplan** – dans ce cas, ONCARE.

TRAITEMENT DES DONNÉES D'ACTIVITÉ

Applicable uniquement si les utilisateurs de votre application connectée consentent et autorisent le transfert de données.

Outils myoncare offre aux **utilisateurs de l'application** la possibilité de connecter le **l'application myoncare** à certaines applications de santé (par exemple AppleHealth, GoogleFit, Withings) ("**Application Santé**»), à condition que ceux-ci soient utilisés par l' **utilisateur de l'application** et la connexion est faite par l' **utilisateur de l'application.** Si la connexion est établie, les données d'activité collectées par l' **application de santé** vous seront fournies dans le but de vous fournir des informations contextuelles supplémentaires concernant l'activité **de l'utilisateur de l'application**. Veuillez noter que les données d'activité ne sont pas validées par **myoncare tools** et ne doit donc pas être utilisé à des fins diagnostiques comme base de décision médicale.

Le traitement des données d'activité relève de la responsabilité de vos patients.

Types de données: Le type et l'étendue des données transférées dépendent de la décision des **utilisateurs de**

l'application. Les données peuvent inclure le poids, la taille, les pas effectués, les calories brûlées, les heures de sommeil, la fréquence cardiaque et la pression artérielle, entre autres.

Finalité du traitement des données d'activité: les données d'activité de l'utilisateur de l'application vous sont fournies dans le but de vous fournir des informations contextuelles supplémentaires concernant l'activité de **l'utilisateur de l'application** . Veuillez noter que les données d'activité ne sont pas validées par **myoncare tools** et ne doit donc pas être utilisé à des fins diagnostiques comme base de décision médicale.

Justification du traitement:
Le responsable des données est le patient lui-même, en vous donnant accès à ses données d'activité dans le but de consulter les informations partagées. Par conséquent, aucune autre justification n'est requise.

TRAITEMENT DES DONNÉES RELATIVES À LA SÉCURITÉ DES PRODUITS

Applicable uniquement si vous utilisez la variante dispositif médical des outils myoncare.

Le **portail myoncare** et l' **application myoncare** sont classés et commercialisés en tant que dispositifs médicaux conformément à la réglementation européenne sur les dispositifs médicaux. En tant que fabricant de l' **outil myoncare**, nous devons respecter certaines obligations légales (par exemple, surveiller les fonctionnalités de l'outil, évaluer les rapports d'incidents qui pourraient être liés à l'utilisation de l'outil, suivre les utilisateurs, etc.). De plus, **les outils myoncare** vous permettent de collecter des données personnelles sur des dispositifs médicaux ou des médicaments spécifiques utilisés dans le traitement de vos patients. Les fabricants de ces dispositifs médicaux ou médicaments ont également des obligations légales en matière de surveillance du marché (par exemple, la collecte et l'évaluation des rapports sur les effets secondaires).
ONCARE est le responsable du traitement des données de sécurité des produits.

Types de données: rapports de cas, données personnelles fournies dans un rapport d'incident et résultats de l'évaluation, coordonnées du déclarant.

Traitement des données de sécurité des produits: Nous stockons et évaluons toutes les données personnelles dans le cadre de nos obligations légales en tant que fabricant d'un dispositif médical et transmettons ces données personnelles (si possible après pseudonymisation) aux autorités compétentes, aux organismes notifiés ou à d'autres responsables du traitement des données ayant des obligations de surveillance. En outre, nous stockerons et transférerons des données personnelles relatives aux dispositifs médicaux et/ou aux médicaments si nous recevons des communications de votre part en tant que rapporteur de ces informations, de votre patient ou d'un tiers (par exemple, nos distributeurs ou importateurs des **outils myoncare** dans votre pays) qui doivent être signalées au fabricant du produit afin que celui-ci puisse se conformer à ses obligations légales en matière de sécurité du produit.

Justification du traitement des données de sécurité du produit :
La base juridique du traitement des données personnelles pour l'exécution d'obligations légales en tant que fabricant de dispositifs médicaux ou de médicaments est l'Art. 6 par. 1 lit. c, art. 9 par. 2 lit.i du RGPD en conjonction avec les obligations de surveillance post-commercialisation en vertu de la législation sur les dispositifs médicaux et de la directive sur les dispositifs médicaux (réglementée à partir du 26 mai 2021 au chapitre VII du nouveau règlement sur les dispositifs médicaux (UE) 2017/745) et/ou de la législation sur les médicaments.

MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Applicable uniquement si vous utilisez les outils myoncare pour le remboursement.

Le **portail myoncare** vous accompagne dans l'initiation de vos procédures standards de remboursement des prestations de santé dispensées à vos patients via l' **application myoncare**. Pour permettre le processus de remboursement, le **portail myoncare** prend en charge la collecte des données personnelles (de santé) de vos patients à partir du **portail myoncare** afin de faciliter la transmission de ces données à l'unité de coûts du patient dans le cadre des processus de remboursement habituels (soit votre Association des médecins de

l'assurance maladie obligatoire, soit la caisse d'assurance maladie du patient). Vous êtes le responsable des données de remboursement et responsable du respect des réglementations en matière de protection des données pour le traitement des données personnelles de vos patients dans le cadre du processus de remboursement. ONCARE agit en tant que sous-traitant des données sur la base de l'accord de traitement des données conclu avec vous en tant que **prestataire de santé**.

Types de données: nom du patient, diagnostic, indications, traitement, durée du traitement, autres données nécessaires à la gestion du remboursement.

Traitement des données de remboursement: En tant qu'agent, vous transmettez les données de traitement du patient nécessaires au remboursement à l'unité de coûts (soit votre association d'assurance maladie, soit la caisse d'assurance maladie du patient) et l'unité de coûts traite les données de remboursement afin de vous rembourser.

Justification du traitement des données de remboursement : Les données de remboursement sont traitées sur la base des §§ 295, 301 SGB V. Le traitement des données par ONCARE pour vous est également effectué sur la base de l'Art. 28 du RGPD (accord de traitement des commandes).

QUELLE EST LA TECHNOLOGIE UTILISÉE PAR LE PORTAIL MYONCARE ET L'APPLICATION MYONCARE ?

Le **portail myoncare** fonctionne comme un outil Web pour lequel vous avez besoin d'une connexion Internet fonctionnelle et de toute version actuelle du navigateur Internet Chrome, Firefox ou Safari.

Service d' E-mail
Nous utilisons Brevo (fourni par Sendinblue GmbH, situé à Köpenicker Straße 126, 10179 Berlin) et Sendgrid (fourni par Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, États-Unis). Ces services d'e-mail peuvent être utilisés pour organiser l'envoi des e-mails. Sendgrid est utilisé pour envoyer des e-mails de confirmation, des confirmations de transaction et des e-mails contenant des informations importantes relatives aux demandes. Les données que vous saisissez dans le but de recevoir des e-mails sont stockées sur les serveurs de Sendgrid. Lorsque nous envoyons des e-mails en votre nom via SendGrid, nous utilisons une connexion sécurisée SSL.
La communication par e-mail est utilisée pour les tâches suivantes :

- Se connecter pour la première fois à l'application web ;
- Réinitialisation du mot de passe de l'application web;
- Créer un compte pour l'application patient;
- Réinitialiser le mot de passe de l'application patient;
- Génération et envoi d'un rapport;
- Remplacer les notifications push par des e-mails pour **PWA** (Progressive Web App) dans les cas suivants:

(i) si un **careplan** se termine dans un jour;
(ii) si un médicament a été attribué;
(iii) si la **politique de confidentialité** a été mise à jour;
(iv) lors de l'envoi d'un rendez-vous à des patients et à des médecins, en particulier pour le type de rendez-vous « appel vidéo »;
v) Toute information relative à une «**CareTask**» ou si un **prestataire de soins de santé** a attribué une **CareTask**.

Brevo (Politique de confidentialité) :
Politique de confidentialité - Protection des données personnelles | Brevo

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

Visible
Il s'agit d'un outil d'analyse Web open source. Matomo (fourni par InnoCraft Ltd., Nouvelle-Zélande) ne transmet pas de données à des serveurs hors du contrôle d'ONCARE. Matomo est initialement désactivé lorsque vous utilisez nos services. Ce n'est que si vous êtes d'accord que votre comportement d'utilisateur sera enregistré de manière anonyme. S'il est désactivé, un « cookie persistant » sera stocké, si les paramètres de votre navigateur le permettent. Ce cookie signale à Matomo que vous ne souhaitez pas que votre navigateur soit enregistré.

Les informations d'utilisation collectées par le cookie sont transmises à nos serveurs et y sont stockées afin que nous puissions analyser le comportement des utilisateurs.
Les informations générées par le cookie concernant votre utilisation sont les suivantes :

- Système d'exploitation de l'utilisateur;
- Géolocalisation de l'utilisateur;
-Navigateur;
-Rôle;
-Adresse IP;
- Sites visités via web / PWA (pour plus d'informations, consultez la section sur les PWA dans cette **Politique de confidentialité**);
- boutons sur lequel l'utilisateur **clique** dans le **portail myoncare,** dans l' **application myoncare** et dans **myoncare PWA**.

Les informations générées par le cookie ne seront pas transmises à des tiers.

Vous pouvez refuser l'utilisation des cookies en sélectionnant les paramètres appropriés dans votre navigateur. Cependant, veuillez noter que vous ne pourrez peut-être pas utiliser toutes les fonctionnalités dans ce cas. Pour plus d'informations, veuillez consulter: https://matomo.org/privacy-policy/

La base juridique du traitement des données personnelles des utilisateurs est l'Art. 6 par. 1 phrase 1 lit. a RGPD. Le traitement des données personnelles des utilisateurs nous permet d'analyser le comportement d'utilisation. En évaluant les données obtenues, nous sommes en mesure de compiler des informations sur l'utilisation des différents composants de nos services. Cela nous aide à améliorer continuellement nos services et leur convivialité.

Nous traitons et stockons les données personnelles uniquement pendant la durée nécessaire à la réalisation de l'objectif visé.

TRANSFERT SÉCURISÉ DES DONNÉES PERSONNELLES

Nous utilisons des mesures de sécurité techniques et organisationnelles appropriées pour protéger de manière optimale les données personnelles que nous stockons contre la manipulation accidentelle ou intentionnelle, la perte, la destruction ou l'accès par des personnes non autorisées. Les niveaux de sécurité sont constamment révisés en collaboration avec des experts en sécurité et adaptés aux nouvelles normes de sécurité.

L'échange de données depuis et vers le portail ainsi que depuis et vers l'application est crypté. Nous proposons SSL comme protocole de cryptage pour une transmission sécurisée des données. L'échange de données est également crypté et s'effectue à l'aide de pseudo-clés.

TRANSFERTS DES DONNÉES / DIVULGATION À DES TIERS

Nous ne transmettrons vos données personnelles à des tiers que dans le cadre des dispositions légales ou sur la base de votre consentement. Dans tous les autres cas, les informations ne seront pas divulguées à des tiers, sauf si nous y sommes obligés en raison de dispositions légales impératives (divulgation à des organismes externes, y compris les autorités de surveillance ou d'application de la loi).

Toute transmission de données personnelles est cryptée lors de la transmission.

Les informations sur la manière dont nous traitons les données personnelles (de santé) de vos patients qui utilisent l' **application myoncare** est résumé dans une **politique de confidentialité** distincte pour **l'application myoncare**. Vous pouvez trouver cette **politique de confidentialité pour les patients** ici. Veuillez également lire cette **politique de confidentialité des patients** soigneusement. Pour une partie du traitement des données des patients, vous êtes le responsable du traitement des données et responsable du respect de la protection des données (par exemple, la transmission des données de traitement au patient).

INFORMATIONS GÉNÉRALES SUR LE CONSENTEMENT AU TRAITEMENT DES DONNÉES

Votre consentement constitue également un consentement au traitement des données en vertu de la loi sur la protection des données. Avant de nous donner votre consentement, nous vous informerons de la finalité du traitement des données et de votre droit d'opposition.
Si le consentement concerne également le traitement de catégories particulières de données à caractère personnel, le **portail myoncare** vous en informera expressément dans le cadre de la procédure de consentement.
Traitement de catégories particulières de données à caractère personnel conformément à l'Art. 9 par. 1 du RGPD ne peut avoir lieu que si cela est nécessaire en raison de dispositions légales et qu'il n'y a aucune raison

de supposer que vos intérêts légitimes s'opposent au traitement de ces données à caractère personnel ou que vous avez donné votre consentement au traitement de ces données à caractère personnel conformément à l'Art. 9 par. 2 du RGPD.
Pour le traitement des données pour lequel votre consentement est requis (comme expliqué dans cette **politique de confidentialité)**, le consentement sera obtenu dans le cadre du processus d'inscription. Une fois l'inscription réussie, les consentements peuvent être gérés dans les paramètres du compte **portail myoncare**. En outre, ONCARE vous demandera d'accepter un accord de traitement des données pour les données traitées par ONCARE sous votre responsabilité en tant que responsable du traitement des données.

DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Dans notre organisation, nous veillons à ce que seules les personnes qui y sont obligées afin de remplir leurs obligations contractuelles et légales soient autorisées à traiter des données personnelles.

Dans certains cas, des prestataires de services assistent nos départements spécialisés dans l'accomplissement de leurs tâches. Les accords de protection des données nécessaires ont été conclus avec tous les prestataires de services qui sont des sous-traitants de données personnelles. Ces fournisseurs de services sont des fournisseurs de stockage cloud de Google (Google Firebase) et des fournisseurs de services d'assistance.

Google Firebase est une « base de données NoSQL » qui permet la synchronisation entre le **portail myoncare** et **l'application myoncare** de votre patient. NoSQL définit un mécanisme de stockage des données qui n'est pas seulement modélisé dans des relations tabulaires en permettant une mise à l'échelle « horizontale » plus facile par rapport aux systèmes de gestion de bases de données tabulaires/relationnelles dans un cluster de machines.

À cet effet, une pseudo-clé du **portail myoncare** et de **l'application myoncare** est stocké dans Google Firebase avec le careplan correspondant. Le transfert de données est pseudonymisé pour ONCARE et ses prestataires de services, ce qui signifie qu'ONCARE et ses prestataires de services ne peuvent pas établir de relation avec vous en tant que personne concernée. Pour ce faire, les données sont cryptées pendant le transfert et utilisent des pseudo-clés pour suivre ces transferts au lieu d'identifiants personnels tels que des noms ou des adresses e-mail. La réidentification a lieu dès que les données personnelles ont atteint le compte du patient dans **l'application myoncare** ou dans votre compte dans le **portail myoncare** après vérification par des tokens spécifiques.

Nos prestataires de stockage dans le cloud offrent un stockage cloud dans lequel est stocké le gestionnaire Firebase, qui gère les URL Firebase pour le **portail myoncare**. De plus, ces prestataires de services fournissent le domaine de serveur isolé du **portail myoncare**, dans lequel vos données personnelles ainsi que celles de votre patient sont stockées. Il héberge également le service de gestion de vidéos et de fichiers de myoncare, qui permet des vidéoconférences cryptées et l'échange de données entre vous et votre patient. L'accès à vos données personnelles par vous et votre patient est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées pendant le transfert et pseudonymisées pour ONCARE et ses prestataires de services pendant le transfert et au repos. Les prestataires de services d'ONCARE n'ont à aucun moment accès à ces données personnelles.

En outre, nous faisons appel à des prestataires de services pour traiter les demandes de service (prestataires de services d'assistance) concernant l'utilisation du compte, par exemple si vous avez oublié votre mot de passe, si vous souhaitez modifier votre adresse e-mail enregistrée, etc. Les accords de traitement des commandes nécessaires ont été conclus avec ces prestataires de services; de plus, les employés chargés du traitement des demandes de service ont été formés en conséquence. À la réception de votre demande de service, un numéro de ticket lui sera attribué.
S'il s'agit d'une demande de service concernant l'utilisation de votre compte, les informations pertinentes que vous nous avez fournies lors de la prise de contact seront transmises à l'un des employés autorisés du service externe. Ils vous contacteront ensuite.

Dans le cas contraire, elles resteront traitées par du personnel ONCARE spécialement agréé, comme décrit dans la section « TRAITEMENT DES DONNÉES OPÉRATIONNELLES ».

Par l'intermédiaire de nos prestataires de services d'assistance, nous utilisons l'outil RepairCode, également connu sous le nom de Digital Twin Code. Il s'agit d'une plateforme d'expérience client permettant de traiter les commentaires externes avec la possibilité de créer des tickets d'assistance. Vous trouverez ici la Politique de confidentialité: https://app.repaircode.de/?main=main-client – Legal/privacy.

Enfin, nous affichons du contenu provenant d'Instagram (fournisseur : Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlande), tel que des images, des vidéos ou des publications. Si vous cliquez sur une publication Instagram liée, vous serez redirigé vers Instagram. Au cours de ce processus, Instagram peut définir des cookies et traiter les données des utilisateurs.
Lorsque vous visitez une page contenant une publication Instagram liée, votre navigateur peut établir automatiquement une connexion aux serveurs d'Instagram. Instagram reçoit ainsi l'information que vous avez visité le site web, même si vous n'avez pas de compte Instagram ou si vous n'êtes pas connecté. Si vous êtes connecté, Instagram peut associer la visite à votre compte utilisateur.
Politique de confidentialité:
https://privacycenter.instagram.com/policy

TRANSFERT DE DONNÉES PERSONNELLES VERS DES PAYS TIERS

Pour fournir nos services, nous pouvons faire appel à des prestataires de services situés en dehors de l'Union européenne (pays tiers). Si les données sont transférées vers un pays tiers où le niveau de protection des données personnelles est jugé insuffisant, nous veillons à ce que des mesures appropriées soient prises conformément au droit national et européen. Si nécessaire, cela inclut la mise en œuvre de clauses contractuelles types entre les parties au traitement.
Les données personnelles collectées par le **portail myoncare** ou **l'application myoncare** ne sont pas stockées dans app stores. Les données personnelles ne seront transférées vers des pays tiers (en dehors de l'Union européenne ou de l'Espace économique européen) que si cela est nécessaire à l'exécution de l'obligation contractuelle, si la loi l'exige ou si vous nous avez donné votre consentement.

La synchronisation du **portail myoncare** avec **l'application myoncare** se déroule à l'aide de Google Firebase. Les serveurs Google Firebase sont hébergés dans l'Union européenne. Néanmoins, conformément aux conditions générales de Google Firebase, un transfert temporaire de données vers des pays dans lesquels Google et les prestataires de services associés ont des succursales est possible ; pour certains services Google Firebase, les données ne sont transférées qu'aux États-Unis, sauf si le traitement a lieu dans l'Union européenne ou l'Espace économique européen. L'accès non autorisé à vos données est empêché par le chiffrement de bout en bout et par les jetons d'accès sécurisé. Nos serveurs en ligne sont hébergés en Allemagne. À des fins d'analyse, les e-mails envoyés avec SendGrid contiennent ce que l'on appelle un « pixel de suivi » qui se connecte aux serveurs de Sendgrid lors de l'ouverture de l'e-mail. Cela peut être utilisé pour déterminer si un e-mail a été ouvert.

Nous intégrons le contenu d'Instagram, fourni par Meta Platforms Ireland Ltd. Si vous cliquez sur une publication Instagram liée, il est possible que des données personnelles (par exemple, l'adresse IP, les informations du navigateur, les interactions) soient transmises à Meta Platforms Inc. aux États-Unis ou dans d'autres pays tiers. Meta est certifié dans le cadre de la réglementation UE-États-Unis. Data Privacy Framework (DPF), qui reconnaît un niveau adéquat de protection des données pour les transferts vers les États-Unis. Toutefois, les données peuvent également être transférées vers des pays pour lesquels il n'existe pas de décision d'adéquation de la Commission européenne. Dans de tels cas, des mesures de protection supplémentaires peuvent être nécessaires, bien que leur efficacité ne puisse pas toujours être entièrement garantie.

Base légale
Le traitement des données est basé sur votre consentement (Art. 6 par. 1 lit. a du RGPD). Vous pouvez révoquer ce consentement à tout moment. La légalité des traitements de données qui ont déjà eu lieu n'est pas affectée par la révocation.

Veuillez noter que nous transmettons généralement vos données à un serveur SendGrid aux États-Unis et y sont stockées. Nous avons conclu un contrat avec Sendgrid qui contient les clauses contractuelles types de l'UE. Cela garantit un niveau de protection comparable à celui de l'UE.

Pour traiter les données d'activité, des interfaces avec les services Google Cloud (dans le cas de GoogleFit) ou avec AppleHealth ou Withings sont utilisées au sein de l'appareil mobile de **l'utilisateur de l'application**. **myoncare tools** utilisent ces interfaces fournies par Google, Apple et Withings, pour demander des données d'activité à partir des applications de santé connectées. L'enquête envoyée par **myoncare tools** ne contient aucune donnée personnelle. Les données personnelles sont mises à la disposition de **myoncare tools** via ces interfaces.

DURÉE DE CONSERVATION DES DONNÉES PERSONNELLES

Nous conserverons vos données personnelles aussi longtemps qu'elles seront nécessaires aux fins pour lesquelles elles sont traitées. Veuillez noter que de nombreuses périodes de conservation nécessitent le stockage continu des données personnelles. Cela s'applique en particulier aux obligations de conservation en vertu du droit commercial ou fiscal.

Veuillez noter qu'ONCARE est également soumis à des obligations de conservation, qui sont convenues contractuellement avec vous sur la base des dispositions légales. De plus, en raison de la classification et, le cas échéant, de votre utilisation du **portail myoncare** et de **l'application MyonCare** en tant que dispositif médical, certaines durées de conservation s'appliquent au portail, qui résultent de la loi sur les dispositifs médicaux. S'il n'y a pas d'autres obligations de conservation, les données personnelles seront systématiquement supprimées dès que l'objectif aura été atteint.

En outre, nous pouvons conserver des données personnelles si vous nous avez donné votre consentement pour le faire ou si un litige survient et que nous utilisons des preuves dans les délais de prescription légaux, qui peuvent aller jusqu'à 30 ans; Le délai de prescription normal est de trois ans.

VOS DROITS EN TANT QUE PERSONNE CONCERNÉE

Diverses données à caractère personnel sont nécessaires à l'établissement, à l'exécution et à la résiliation de la relation contractuelle ainsi qu'à l'exécution des obligations contractuelles et légales qui y sont liées. Il en va de même pour l'utilisation de notre **Portail MyonCare** et les différentes fonctions qu'il offre.

Dans certains cas, les données personnelles doivent également être collectées ou mises à disposition conformément aux dispositions légales. Veuillez noter que sans fournir ces données personnelles, il n'est pas possible de traiter votre demande ou de remplir l'obligation contractuelle sous-jacente.

DÉCISIONS AUTOMATISÉES DANS DES CAS INDIVIDUELS

Nous n'utilisons pas de traitement purement automatisé pour prendre des décisions.

VOS DROITS EN TANT QUE PERSONNE CONCERNÉE

Nous souhaitons vous informer de vos droits en tant que personne concernée. Ces droits sont énoncés aux articles 15 – 22 du RGPD et comprennent :

Droit d'accès (Art. 15 du RGPD) : Vous avez le droit de demander des informations sur la manière dont vos données personnelles sont traitées, y compris des informations sur les finalités du traitement, les destinataires, la durée de stockage, ainsi que vos droits de rectification, de suppression et d'opposition. Vous avez également le droit de recevoir une copie de toutes les données personnelles que nous détenons à votre sujet.

Droit à l'effacement / droit à l'oubli (Art. 17 du RGPD) : Vous pouvez nous demander de supprimer vos données personnelles collectées et traitées par nos soins dans les meilleurs délais. Dans ce cas, nous vous demanderons de supprimer le **portail myoncare** depuis votre ordinateur. Veuillez toutefois noter que nous ne pouvons supprimer vos données personnelles qu'après l'expiration des délais de conservation légaux.

Droit de rectification (Art. 16 du RGPD) : Vous pouvez nous demander de mettre à jour ou de corriger des données personnelles inexactes vous concernant ou de compléter des données personnelles incomplètes.

Droit à la portabilité des données (Art. 20 du RGPD) : En principe, vous pouvez demander que nous vous fournissions les données personnelles que vous nous avez fournies et qui sont traitées automatiquement sur la base de votre consentement ou de l'exécution d'un contrat avec vous sous une forme lisible par machine afin qu'elles puissent être « portées » à un prestataire de services de remplacement.

Droit à la limitation du traitement des données (Art. 18 du RGPD) : Vous avez le droit de demander la limitation du traitement de vos données personnelles si la précision des données est contestée, si le traitement est illégal, si les données sont nécessaires à des actions en justice ou si une opposition au traitement est en cours d'examen.

Droit d'opposition au traitement des données (Art. 21 du RGPD) : Vous avez le droit de vous opposer à l'utilisation de vos données personnelles et de retirer votre consentement à tout moment si nous traitons vos données personnelles sur la base de votre consentement. Nous continuerons à fournir nos services s'ils ne dépendent pas du retrait du consentement.
Pour exercer ces droits, veuillez nous contacter à l'adresse suivante : privacy@myoncare.com. L'opposition et la révocation du consentement doivent être déclarées sous forme de texte à privacy@myoncare.com .
Nous vous demanderons de fournir une preuve suffisante de votre identité pour nous assurer que vos droits sont protégés et que vos données personnelles ne seront divulguées qu'à vous et non à des tiers.

N'hésitez pas à nous contacter à tout moment au privacy@myoncare.com Si vous avez des questions sur le traitement des données dans notre entreprise ou si vous souhaitez retirer votre consentement. Vous avez également le droit de contacter l'autorité de contrôle compétente en matière de protection des données.

CONTRÔLEUR DE LA PROTECTION DES DONNÉES

Vous pouvez contacter notre délégué à la protection des données pour répondre à toutes vos questions sur la protection des données à l'adresse privacy@myoncare.com.

MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Nous nous réservons expressément le droit de modifier cette **politique de confidentialité** à l'avenir, à notre seule discrétion. Des modifications ou des ajouts peuvent être nécessaires, par exemple, pour répondre à des exigences légales, pour se conformer à l'évolution technique et économique ou pour répondre aux intérêts de **l'application** ou **les utilisateurs du portail**.

Des modifications sont possibles à tout moment et vous seront communiquées de manière appropriée et dans un délai raisonnable avant qu'elles n'entrent en vigueur (par exemple, en publiant une **politique de confidentialité** lors de la connexion ou en prévenant à l'avance des modifications importantes).

ONCARE GmbH

Adresse postale

Balanstraße 71a

81541 Munich, Allemagne

L | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Coordonnées du délégué à la protection des données

privacy@myoncare.com

En cas de questions d'interprétation ou de litiges, seule la version allemande de la politique de confidentialité est contraignante et fait foi.

Dernière mise à jour le 20 Février 2025.
* * * *

États-Unis Politique de confidentialité POLITIQUE DE CONFIDENTIALITÉ

Bienvenue sur myoncare, le portail de santé numérique pour des soins efficaces et adaptés aux besoins des patients.
Pour nous, chez Oncare GmbH (ci-après dénommée «**ONCARE"** ou «**nous**", **"Nous**", "**notre**"), la protection de votre vie privée et de toutes les données personnelles vous concernant lors de l'utilisation du portail myoncare est d'une grande importance. Nous sommes conscients de la responsabilité qui découle de la mise à disposition et de l'enregistrement de vos données personnelles sur le portail myoncare. Par conséquent, nos systèmes technologiques utilisés pour les services myoncare sont configurés selon les normes les plus élevées et le traitement légal des données est au cœur de notre compréhension éthique en tant qu'entreprise.

Nous traitons vos données personnelles conformément aux dispositions légales applicables en matière de protection des données personnelles. Dans la présente politique de confidentialité, vous découvrirez pourquoi et comment ONCARE traite vos données personnelles que nous collectons auprès de vous ou que vous nous fournissez lorsque vous décidez d'utiliser le portail myoncare. En particulier, vous trouverez une description des données personnelles que nous collectons et traitons, ainsi que la finalité et la base sur lesquelles nous traitons les données personnelles et les droits dont vous disposez.

Tous les renseignements que nous détenons et qui sont fournis par vos prestataires de soins de santé sont **des informations de santé protégées (PHI)** et/ou d'autres informations médicales. Ceux-ci sont protégés par certaines lois, telles que la loi sur la transférabilité et l'obligation redditionnelle en matière d'assurance-santé (**HIPAA)** des États-Unis. Nous avons l'obligation légale de protéger la confidentialité et la sécurité des informations de santé protégées. Nous nous efforçons constamment de protéger les informations de santé par des moyens administratifs, physiques et techniques, et nous nous conformons par ailleurs aux lois fédérales et étatiques applicables.

Veuillez lire attentivement la politique de confidentialité pour vous assurer que vous comprenez chaque disposition. Après avoir lu la politique de confidentialité, vous aurez la possibilité de consentir à la politique de confidentialité et de consentir au traitement de vos données personnelles comme décrit dans la politique de confidentialité. Si vous donnez votre consentement, la politique de confidentialité fait partie du contrat entre vous et ONCARE.

En cas de questions d'interprétation ou de litiges, seule la version allemande de la politique de confidentialité est contraignante et fait foi.

DÉFINITIONS
« Utilisateur de l'application» désigne tout utilisateur de l'Application myoncare (votre patient).

«Technologie blockchain» Le système myoncare contient une base de données décentralisée supplémentaire dans laquelle sont stockées les données de toutes les installations.

«**Prestataire de careplan**» désigne vous ou tout autre prestataire de services ou tiers (par exemple, un fabricant de dispositifs médicaux, une société pharmaceutique) qui met des careplans à la disposition d'autres utilisateurs du portail via le myoncare Store ou d'autres moyens d'échange de données.

«**Utilisateur du careplan**» désigne vous ou tout autre prestataire de services (Utilisateur du Portail) qui utilise un Plan de Soins (« Parcours ») pour le traitement de ses Patients enregistrés.

«Pathway» est un plan de traitement standardisé qui peut déterminer les étapes du diagnostic et des thérapies. **"Caretasks"** sont des tâches ou actions spécifiques au sein d'un parcours qui doivent être réalisées par les prestataires de soins concernés, le personnel soignant ou le patient lui-même.

"**Règlement général sur la protection des données de l'UE**". Le Règlement général sur la protection des données (RGPD) est une loi européenne sur la protection des données. Le règlement est entré en vigueur le 25 mai 2018 et vise à harmoniser la protection des données dans tous les États membres et à donner aux citoyens plus de contrôle sur leurs données personnelles. Le RGPD s'applique à toutes les entreprises et organisations qui opèrent dans l'UE ou traitent des données

personnelles de citoyens de l'UE, que l'entreprise soit située à l'intérieur ou à l'extérieur de l'UE. Le RGPD s'applique également à vous en tant que citoyen américain, car ONCARE est basé en Allemagne.

"**Prestataire de soins de santé**» désigne vous ou tout autre médecin, clinique, établissement de santé ou autre professionnel de la santé agissant seul ou en votre nom ou au nom d'un autre médecin, d'une clinique ou d'un établissement de santé (l'utilisateur visé).

"**Informations sur la santé**» désigne toutes les informations, y compris les informations génétiques, qu'elles soient enregistrées oralement, sous quelque forme ou sur tout support, qui
- sont traitées ou transférées par un prestataire de soins de santé, un régime de santé, une autorité sanitaire, un employeur, un assureur-vie, une école ou une université, ou un centre d'information sur la santé; et
- se rapportent à la santé physique ou mentale passée, présente ou future d'une personne ou à un état de santé également lié au traitement médical de la personne ;
- la rémunération passée, présente ou future des soins de santé d'une personne.

« Informations de santé protégées » ou **« PHI »** désigne les renseignements sur la santé permettant d'identifier une personne qui (i) sont transmis par voie électronique ; (ii) sont conservés sur des supports électroniques ; ou (iii) transmis ou conservé sous toute autre forme ou support.

"**Loi sur la transférabilité et l'obligation redditionnelle en matière d'assurance-santé**," "**HIPAA.** La Health Insurance Portability and Accountability Act de 1996 (HIPAA) est une loi américaine. Loi fédérale qui comprend la création de normes nationales pour protéger les renseignements sensibles sur la santé des patients contre la divulgation non autorisée sans leur consentement ou à leur insu. Les exigences de la loi HIPAA s'appliquent à l'utilisation et à la divulgation des informations de santé des personnes par les institutions soumises à la loi HIPAA. Ces personnes et organisations sont appelées « entités couvertes ».

«**L'application myoncare**» désigne l'application mobile myoncare à l'usage des patients qui souhaitent utiliser les services proposés par Oncare.

«**myoncare Store**» est la plateforme exploitée par ONCARE qui fournit des concepts de soins numériques (careplans) pour le traitement de vos patients inscrits via le portail myoncare.

«**Portail myoncare**» est le portail web myoncare, qui est destiné à un usage professionnel par les utilisateurs du portail et sert d'interface entre les utilisateurs du portail et les patients en tant **qu'utilisateurs de l'application.**

«**L'application myoncare PWA**» désigne l'application myoncare Progressive Web App pour les patients qui souhaitent utiliser les services proposés par Oncare via l'application PWA et non via l'application myoncare.

«**myoncare Tools**» désigne l'application myoncare et le portail myoncare ensemble.

«**Services de myoncare**» désigne les services, fonctionnalités et autres offres qui sont ou pourraient être proposés aux utilisateurs du portail via le portail myoncare et/ou au **utilisateurs de l'application** via l'application myoncare.

«**Oncare**» désigne ONCARE GmbH, Allemagne.

«**Utilisateur du portail**» désigne vous ou tout autre prestataire de services utilisant le portail Web myoncare.

ONCARE est un « partenaire commercial » tel que défini par la HIPAA et fournit des services aux prestataires de soins de santé et aux régimes de santé. Ces services sont fournis aux entités désignées comme « entités couvertes » par la loi HIPAA ; ONCARE conclut des accords correspondants avec ces institutions.
Conformément à nos conditions d'utilisation, notre offre s'adresse uniquement aux patients âgés de 18 ans et plus. Par conséquent, aucune donnée personnelle d'enfants et d'adolescents de moins de 18 ans n'est stockée et traitée.

«**Politique de confidentialité**» désigne la présente déclaration qui vous est fournie en tant qu'utilisateur du Portail myoncare, qui décrit la manière dont nous recueillons, utilisons et stockons vos informations personnelles et vous informe de vos droits généraux.

«**Conditions d'utilisation**» désigne les conditions d'utilisation pour l'utilisation du Portail myoncare.

RESPECT DES LOIS

Oncare GmbH, une société enregistrée au Tribunal de District de Munich sous le numéro d'enregistrement 219909 dont le siège social est situé Balanstraße 71a, 81541 Munich, Allemagne, propose et exploite le portail web interactif **Portail myoncare** (pour les professionnels de santé) et l'application mobile **myoncare App** (pour les patients) comme accès aux **services myoncare**. Cette **politique de confidentialité** s'applique à toutes les données à caractère personnel traitées par ONCARE dans le cadre de l'utilisation du **portail myoncare**. Pour l'utilisation de **l'application myoncare** par les patients, vous trouverez **ici** une politique de confidentialité distincte pour les patients.

ONCARE est un « business partner » (business partner en termes de **HIPAA**) qui fournit des services et des régimes de santé aux **prestataires de soins de santé**, appelées « entités couvertes » au sens de la HIPAA ; ONCARE conclut des accords de partenariat commercial avec ces entreprises couvertes. ONCARE n'utilisera et ne divulguera **PHI** que conformément aux accords de partenariat commercial et à la**HIPAA**.

La loi américaine nous oblige à respecter les lois conçues pour protéger la confidentialité et la sécurité des informations de santé protégées. Nous vous informerons immédiatement si une violation (appelée violation de données) se produit qui aurait pu mettre en danger la confidentialité ou la sécurité des informations (de santé).

QU'EST-CE QU'UNE DONNÉE PERSONNELLE AU SENS DU RGPD ?

«**Données personnelles**» désigne toute information permettant d'identifier une personne physique. En particulier, cela inclut, mais sans s'y limiter, votre nom, votre date de naissance, votre adresse, votre numéro de téléphone, votre adresse e-mail et votre adresse IP.

«**Données de santé**» désigne les données personnelles relatives à la santé physique et mentale d'une personne physique, y compris la fourniture de services de santé qui divulguent des informations sur son état de santé.

Les données doivent être considérées comme «**anonymes**" si aucun lien personnel avec la personne/l'utilisateur ne peut être établi. En revanche, les données «**pseudonymisé**» sont des données à partir desquelles une référence personnelle ou des informations personnellement identifiables sont remplacées par un ou plusieurs identifiants artificiels ou pseudonymes, mais qui peuvent généralement être réidentifiées par la clé d'identification (au sens de l'Art. 4 n° 5 du RGPD).

Application myoncare PWA

Une application web progressive (PWA) est un site web qui a l'apparence et les fonctionnalités d'une application mobile. Les PWA sont conçues pour tirer parti des fonctionnalités natives des appareils mobiles sans avoir besoin d'un app store. L'objectif des PWA est de combiner la différence entre les applications et le Web traditionnel en apportant les avantages des applications mobiles natives dans le navigateur. La PWA est basée sur la technologie de « React ». « React » est un logiciel open-source pour les applications PWA.

Pour utiliser l'application myoncare PWA, les patients ont besoin d'un ordinateur ou d'un smartphone et d'une connexion Internet active. Il n'est pas nécessaire de télécharger une application.

Certains des services de l'application myoncare ne peuvent pas être utilisés dans l'application myoncare PWA, voir la description ci-dessous pour plus de détails. Il s'agit des services ou spécifications suivants :
-Discuter avec des **prestataires de soins de santé**;
-Vidéo;
- Code PIN de sécurité;
-Suivi des données d'activité (par exemple via AppleHealth, GoogleFit, Withings).

Les informations suivantes sur **l'application myoncare** s'appliquent également à **l'application myoncare PWA**, sauf indication contraire dans cette section.

QUELLES DONNÉES PERSONNELLES SONT UTILISÉES LORS DE L'UTILISATION DE L'APPLICATION MYONCARE

Nous pouvons traiter les catégories de données suivantes vous concernant lors de l'utilisation de **l'application myoncare :**

Données opérationnelles: Données personnelles qui nous sont fournies lorsque vous vous inscrivez et vous connectez à notre **portail myoncare,** vous nous contactez au sujet de problèmes avec le portail ou lorsque vous interagissez avec nous dans le but d'utiliser le portail;

Données de traitement : Vous collectez des données personnelles de vos patients, telles que le nom, l'âge, la taille, le poids, l'indication, les symptômes de la maladie et d'autres informations en relation avec le traitement de vos patients dans le **portail myoncare** (par exemple, les données de traitement sont des données personnelles de vos patients qui sont collectées ou traitées lorsque vous contactez votre patient via le **portail myoncare** interactive); Les données d'activité de vos patients connectés seront mises à votre disposition dans votre **portail myoncare**.

Données de magasin commercial: Données personnelles que nous traitons lorsque vous utilisez **myoncare store** soit en tant qu'auteur de **careplan** ou en tant qu'acheteur de **careplan**. L'utilisation de **myoncare store** nécessite le traitement de votre nom et de vos coordonnées ainsi que de vos données de paiement (données de paiement uniquement si un **careplan** est payant).

Données d'activité: Données personnelles que nous traitons lorsqu'un **utilisateur de l'application** connecte **l'application myoncare** à une application de santé (par exemple AppleHealth, GoogleFit, Withings). Les informations sur l'activité de vos patients affiliés sont à votre disposition sur le **portail myoncare**.

Données de recherche commerciales et non commerciales: Nous traitons vos données personnelles sous forme anonymisée/pseudonymisée afin d'analyser et de préparer des rapports scientifiques de synthèse afin d'améliorer les produits, les traitements et les résultats scientifiques.

Données de sécurité du produit: Données personnelles qui sont traitées pour se conformer à nos obligations légales en tant que fabricant de **l'application myoncare** en tant que dispositif médical. En outre, vos données personnelles peuvent être traitées en tant que signalement d'incident pour répondre à des fins de sécurité juridique ou de vigilance d'entreprises de dispositifs médicaux ou pharmaceutiques.

Données de remboursement: Données personnelles nécessaires au processus de remboursement.

TECHNOLOGIE BLOCKCHAIN

Technologie blockchain ("**Chaîne de blocs**") (brevet européen n° 4 002 787) est un service facultatif qui n'est pas obligatoire. C'est à vous, le **prestataire de soins de santé**, de décider d'utiliser la solution blockchain. La **blockchain** est basé sur la technologie d'Hyperledger Fabric. Hyperledger Fabric est un logiciel open source pour les implémentations de blockchain au niveau de l'entreprise. Il offre une plateforme évolutive et sécurisée qui prend en charge les projets blockchain.

La **blockchain** dans le système myoncare se trouve une base de données supplémentaire qui stocke les données de l'application. Toutes les données de la blockchain sont stockées en République Fédérale d'Allemagne. Il s'agit d'une **blockchain** privée ("**Blockchain privée**"), il ne permet que la saisie de participants vérifiés sélectionnés et il est possible d'écraser, de modifier ou de supprimer des entrées selon les besoins.

En général, la **blockchain** se compose de données numériques dans une chaîne de paquets appelés «blocs» qui stockent les transactions correspondantes. La façon dont ces blocs sont reliés les uns aux autres est chronologique. Le premier bloc créé est appelé bloc de genèse, et chaque bloc ajouté par la suite a un hachage cryptographique lié au bloc précédent, ce qui permet de retracer les transactions et les modifications d'informations jusqu'au bloc de genèse. Toutes les transactions à l'intérieur des blocs sont validées et vérifiées par le biais d'un mécanisme de consensus blockchain afin de s'assurer que chaque transaction reste inchangée.

Chaque bloc contient la liste des transactions, un horodatage, son propre hachage et le hachage du bloc précédent. Un hachage est une fonction qui convertit des données numériques en une chaîne

alphanumérique. Dans ce cas, le bloc ne peut plus être synchronisé avec les autres. Si une personne non autorisée tente de modifier les données d'un seul bloc, le hachage du bloc changera également et le lien vers ce bloc sera perdu. Si tous les nœuds (nœuds du réseau) tentent de synchroniser leurs copies, il est déterminé qu'une copie a été modifiée et le réseau considère que ce nœud est défectueux. Ce processus technique empêche les personnes non autorisées de manipuler le contenu de la chaîne blockchain.

Notre **blockchain** est une **blockchain** privée. Une **blockchain** privée est décentralisée. Il s'agit d'un système dit de registre distribué (système numérique d'enregistrement des transactions), qui fonctionne comme une base de données fermée. Contrairement aux **blockchains** publiques, qui sont « non autorisés », les **blockchains** privés sont « autorisés » parce qu'une autorisation est requise pour devenir un utilisateur. Contrairement aux **blockchains** publiques, qui sont accessibles à tous, l'accès aux **blockchains** privés dépend de l'autorisation pour devenir un utilisateur. Cette structure permet de tirer parti de la sécurité et de l'immuabilité de la **technologie blockchain** tout en étant conforme à la protection des données, et de se conformer à la réglementation du Règlement général sur la protection des données (RGPD). Les enregistrements privés de la blockchain peuvent être modifiés ou supprimés; la suppression dans ce contexte signifie que la valeur de référence à l'UUID (Universally unique identifier) dans la base de données du **fournisseur de soins de santé** est supprimée. De plus, le hachage est anonymisé dans la base de données blockchain, de sorte que ce processus global est conforme au règlement général sur la protection des données et que les droits d'une personne concernée sont garantis (droit à l'effacement « droit à l'oubli », Art. 17 du RGPD).

Type de données stockées et traitées dans la blockchain :

-UUID du patient
-Institutions/Leistungserbinger UUID
-UUID du fichier
-Hachage des données de **caretask** et de fichier.
(*UUID : Identifiant Unique Universel*).

Les données stockées dans le **blockchain** sont pseudo-anonymisées.
Notre **blockchain** est conçu pour garantir la confidentialité des données en termes d'intégrité des données, de profil du patient, d'e fichiers et de **CareTasks** et des médicaments assignés. Pour communiquer avec le **blockchain**, l'utilisateur doit enregistrer une série de clés publiques-privées. Le processus d'enregistrement génère des certificats qui sont stockés dans une base de données distincte du **fournisseur de soins** et sur le téléphone mobile du patient. Une copie de sauvegarde de la clé du patient est cryptée et stockée dans la base de données du **fournisseur de soins**, accessible uniquement au patient.

Lors de la vérification du consentement à la protection des données, dans le cas où le **fournisseur de soins de santé** souhaite communiquer avec le patient, le système vérifie si le patient a donné son consentement à la politique de confidentialité du prestataire. La **blockchain** sert donc à assurer l'intégrité et la responsabilité du dossier afin de s'assurer que le patient a accepté la politique de confidentialité.

Lorsqu'un **Fournisseur de soins de santé** télécharge une nouvelle version d'une politique de confidentialité, le hachage du fichier est stocké dans le **blockchain,** et une fois que le patient a accepté la politique de confidentialité, cette interaction est stockée dans le **blockchain.** Chaque fois qu'il communique avec le patient, le **Chaîne de blocs** répond en comparant le hachage avec un indicateur qui indique si le consentement du patient est toujours valide pour la politique de confidentialité actuelle.

En cas de synchronisation du patient, l'intégrité du profil du patient est également assurée par la blockchain. Le **fournisseur de services** Détecte immédiatement si le profil du patient ne se synchronise pas ou ne correspond pas au profil sur le téléphone mobile en comparant le hachage du profil du patient dans le **Chaîne de blocs**. De cette façon, le **fournisseur** de santéatteint une actualité suffisante en ce qui concerne le profil du patient.

Portail myoncare:
Si le **fournisseur de services** décide d'utiliser la solution blockchain, ONCARE met en œuvre un outil supplémentaire, appelé « Adapter Service », qui sert à

communiquer avec la **blockchain.** L'instance blockchain est hébergée par ONCARE.

L'application myoncare:
Les patients peuvent se connecter à la même instance de blockchain à l'aide de l'outil Phone Manager, qui est également hébergé par ONCARE. Ce service est également hébergé par ONCARE.

Justification du traitement : Le traitement des données par ONCARE pour le compte du **prestataire de soins de santé** est effectué sur la base de l'art. 28 du RGPD (accord de traitement des commandes).

TRAITEMENT DES DONNÉES OPÉRATIONNELLES

Si vous êtes une personne de contact pour le fonctionnement du **Portail MyonCare** sur votre site/cabinet (par exemple, administrateur informatique, professionnel de la santé désigné), vous pouvez nous fournir certaines données personnelles lorsque vous nous contactez pour comprendre ou discuter des fonctionnalités et de l'utilisation du **Portail MyonCare**, ou en cas de demande de service.

En cas de demande de service, les données personnelles suivantes peuvent également être consultées par les employés autorisés d'ONCARE :
Vos données personnelles que vous nous avez fournies pour l'inscription et/ou la connexion à notre portail (par exemple, nom, date de naissance, photo de profil, coordonnées).

Les employés autorisés d'ONCARE qui peuvent accéder à votre base de données dans le but de traiter une demande de service sont contractuellement tenus de garder tous les renseignements personnels strictement confidentiels.

Explications importantes sur les notifications push et les e-mails
Dans le cadre de votre soutien par myoncare, nous souhaitons vous informer de la manière dont nous traitons les notifications et les informations importantes que nous vous envoyons.

1. **Notifications push**:
    - Nous vous envoyons des notifications push via notre **myoncare PWA** (Progressive Web App) et l' **application myoncare** pour vous informer sur les tâches, les rendez-vous et les mises à jour importantes.
    - Vous avez la possibilité de désactiver ces notifications push dans les paramètres de votre application.
2. **Notifications par e-mail**:
    - Que vous ayez activé ou désactivé les notifications push, nous continuerons à vous envoyer des informations importantes et des rappels par e-mail.
    - Cela vous permet de ne manquer aucune notification importante et de garantir le bon déroulement de votre assistance.

Pourquoi nous faisons cela :

- Notre objectif est que vous soyez toujours informé de vos tâches et des mises à jour importantes afin de soutenir de manière optimale vos soins.
- Les e-mails sont un moyen fiable de s'assurer que des informations importantes vous parviennent, même lorsque les notifications push sont désactivées.

Vos options d'action :

- Si vous ne souhaitez pas recevoir de notifications push, vous pouvez les désactiver dans les paramètres de l' **application myoncare**
- Veuillez vous assurer que votre adresse e-mail est exacte et à jour pour assurer la bonne réception de nos messages.
- Si vous ne souhaitez pas recevoir de rappels par e-mail, vous pouvez les désactiver dans les paramètres de l'icône **application myoncare.**

Période de conservation
Les données que vous nous fournissez pour recevoir des e-mails seront stockées par nous jusqu'à ce que vous vous déconnectiez de nos services et seront supprimées de nos serveurs et des serveurs de Sendgrid après votre déconnexion.

Lors du traitement des données opérationnelles, ONCARE agit en tant que contrôleur de données responsable du traitement légal de vos données personnelles.

Types de données : adresse e-mail, date de naissance, date d'inscription, votre adresse IP, pseudo-clés générées par le Portail.

L'application utilise l'API Google Maps pour utiliser les informations géographiques. Pendant l'utilisation de google Maps, Google collecte, traite et utilise également les données relatives à l'utilisation des fonctions de cartes. Vous trouverez des informations plus détaillées sur l'étendue, la base juridique et la finalité du traitement des données par Google ainsi que sur la durée de conservation dans la politique de confidentialité de Google.

Finalité du traitement des données opérationnelles: Nous utilisons les données opérationnelles pour maintenir les fonctionnalités du **portail myoncare** et de vous contacter directement si nécessaire ou à votre initiative (par exemple en cas de modifications des conditions d'utilisation, d'assistance nécessaire, de problèmes techniques, etc.). En outre, les données personnelles (adresse e-mail) sont nécessaires et traitées dans le cadre de l'authentification à deux facteurs chaque fois que vous vous connectez au **portail myoncare**.
Justification du traitement: Le traitement des données opérationnelles est justifié sur la base de l'Art. 6 par. 1 lit. b RGPD pour l'exécution du contrat que vous concluez avec ONCARE dans le but d'utiliser le **portail myoncare**.

GÉOLOCALISATION IP

Géolocalisation IP : Nous utilisons une application de géolocalisation pour nos Services. Nous utilisons ipapi (fourni par apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Vienne, Autriche) et Geoapify (fourni par Keptago Ltd., N. Nikolaidi et T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Chypre) pour identifier la localisation des patients utilisateurs. Nous les utilisons pour sécuriser nos applications et pour vérifier la localisation de l'utilisateur patient afin de nous assurer que l'utilisation de nos services est conforme. Nous ne combinons pas les informations que nous recueillons avec d'autres informations sur l'utilisateur qui pourrait les identifier. Les données traitées par apilayer comprennent l'adresse IP du patient et d'autres détails sur la localisation. La base juridique de l'utilisation est l'Art. 6 par. 1 lit. f RGPD. Les données seront supprimées lorsque la finalité associée pour laquelle elles ont été collectées n'existe plus et qu'il n'y a plus d'obligation légale de les stocker. Pour plus d'informations sur leur politique de confidentialité, veuillez consulter https://ipapi.com/privacy/ et Politique de confidentialité | Plateforme de localisation Geoapify.

TRAITEMENT DES DONNÉES OPÉRATIONNELLES

En utilisant le **portail myoncare**, vous saisissez les données personnelles (de santé) de vos patients dans le **portail myoncare** (ex : mise à disposition d'un careplan individualisé, rappel de la prise de médicaments, etc.). De plus, vous et vos patients pouvez télécharger des documents et des fichiers dans le **portail myoncare** et les partager les uns avec les autres. De plus, des fonctions de localisation peuvent être générées et mises en œuvre :

- Ajout d'un lieu ;
- Mise en ligne du logo du site;
- Ajout des détails de l'emplacement ;
- Ajout d'une politique de confidentialité

Il est possible de créer d'autres exigences de consentement pour le patient, pour lesquelles le patient doit donner son consentement afin de se connecter au site Web.
Une politique de confidentialité téléchargée sera affichée à chaque patient qui se connecte au site Web. Toutes les déclarations de consentement doivent être documentées dans la politique de confidentialité téléchargée. Une fois qu'une politique de confidentialité a été téléchargée, elle ne peut être remplacée que par une nouvelle version, mais ne peut pas être supprimée.
Les fichiers sont stockés dans une base de données cloud en Allemagne. Vous pouvez autoriser le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de votre établissement à des fins médicales. Les autres **utilisateurs du portail** n'ont pas accès à ces fichiers.

Par ailleurs, vous pouvez impliquer un **prestataire de soins** extérieur à votre établissement (prestataire de

soins de santé consultant) dans le traitement de vos patients, à condition que vous estimez qu'un avis d'expert supplémentaire serait bénéfique au traitement.

Conformément au RGPD, vous êtes responsable du traitement des données de santé des patients dans le cadre de l'utilisation des services myoncare en tant que responsable des données.

Nous traitons ces données personnelles, y compris les données de santé du patient, dans le cadre d'un accord avec vous et conformément à vos instructions.

Règles du RGPD

Dans le cadre de l'utilisation des services myoncare avec les données de santé des patients, vous êtes donc le responsable du traitement des données (conformément au RGPD). Veuillez ne traiter les données de vos patients que si vous avez obtenu le consentement requis de ces patients. ONCARE agira en tant que sous-traitant (conformément au RGPD) conformément à l'accord de traitement des données distinct que nous avons conclu avec vous sur la base de l'art. 28 du RGPD.

TRAITEMENT DES DONNÉES DE STORE COMMERCIAUX

Applicable uniquement si vous utilisez le myoncare Store en tant qu'utilisateur de Careplan.

Le **myoncare store** est intégré dans le **portail myoncare** et propose l'achat de **careplans**. Après vous être inscrit sur le **portail myoncare**, vous pouvez vous connecter au **myoncare store** à l'aide de vos données de connexion. Vous pouvez utiliser **myoncare store** pour acheter des careplans en tant qu'utilisateur.

Données de l'utilisateur du careplan :
Les données de **l'utilisateur du careplan**, que **myoncare store** traite au cours de son utilisation, sont traitées pour la conclusion d'un contrat de licence avec le **fournisseur du careplan** – dans ce cas ONCARE – et, si des frais sont dus, pour le traitement et le contrôle de l'opération de paiement entre **le fournisseur du careplan** – en l'occurrence ONCARE – et **l'utilisateur du careplan**.

Types de données: nom, coordonnées, coordonnées bancaires.

Traitement des données des magasins commerciaux: Données personnelles que nous traitons dans le cadre de l'utilisation de myoncare store, soit dans le cadre de la paternité de plans de soins, soit dans le cadre de l'achat de plans de soins. En outre, les données de paiement (si des frais d'utilisation sont facturés) seront transmises au **prestataire de careplan**.

Règles du RGPD

Justification du traitement des données des magasins commerciaux : La base juridique du traitement des données à caractère personnel est le contrat de traitement des commandes séparé que nous avons conclu avec le **Fournisseur de plans de soins** sur la base de l'art. 28 du RGPD.

TRAITEMENT DES DONNÉES D'ACTIVITÉ

Applicable uniquement si les utilisateurs de votre application connectée consentent au transfert de données et l'autorisent.

Outils myoncare offre aux **utilisateurs de l'application** la possibilité de connecter l' **application myoncare** à certaines applications de santé (par exemple AppleHealth, GoogleFit, Withings) ("**Application Santé**»), à condition que ceux-ci soient utilisés par l' **utilisateur de l'application** et la connexion est faite par l' **utilisateur de l'application.** Si la connexion est établie, les données d'activité collectées par l' **application de santé** vous seront fournies dans le but de vous fournir des informations contextuelles supplémentaires concernant l'activité **de l'utilisateur de l'application**. Veuillez noter que les données d'activité ne sont pas validées par **les outils myoncare** et ne doivent pas être utilisées aux fins de diagnostic ou comme base pour la prise de décisions cliniques.

Le traitement des données d'activité relève de la responsabilité de vos patients.

Types de données : Le type et l'étendue des données transférées dépendent de la décision des **utilisateurs de l'application.** Les données peuvent inclure le poids, la taille, les pas effectués, les calories brûlées, les heures

de sommeil, la fréquence cardiaque et la pression artérielle, entre autres.

Finalité du traitement des données d'activité : Les données d'activité de l'utilisateur de l'application vous sont fournies dans le but de fournir des informations contextuelles supplémentaires concernant les activités de l'**utilisateur de l'application** . Veuillez noter que les données d'activité ne sont pas validées par **les outils myoncare** et ne doivent pas par conséquent être utilisées aux fins de diagnostic ou comme base pour la prise de décisions cliniques.

Justification du traitement :
Le responsable des données est le patient lui-même en vous donnant accès à ses données d'activité dans le but d'examiner les informations partagées. Par conséquent, aucune autre justification n'est requise.

TRAITEMENT DES DONNÉES RELATIVES À LA SÉCURITÉ DES PRODUITS

***Applicable uniquement si vous utilisez la variante dispositif médical des outils myoncare*.**

Le **portail myoncare** et l' **application myoncare** sont classés et commercialisés en tant que dispositifs médicaux conformément à la réglementation européenne sur les dispositifs médicaux. En tant que fabricant du **Outil MyonCare**, nous devons respecter certaines obligations légales (par exemple, surveiller les fonctionnalités de l'outil, évaluer les rapports d'incidents qui pourraient être liés à l'utilisation de l'outil, suivre les utilisateurs, etc.). De plus, **Outils MyonCare** vous permettre de collecter des données personnelles sur des dispositifs médicaux ou des médicaments spécifiques utilisés dans le traitement de vos patients. Les fabricants de ces dispositifs médicaux ou médicaments ont également des obligations légales en matière de surveillance du marché (par exemple, la collecte et l'évaluation des rapports sur les effets secondaires).

ONCARE est le responsable du traitement des données de sécurité des produits.

Types de données :rapports de cas, données personnelles fournies dans un rapport d'incident et résultats de l'évaluation, coordonnées du déclarant.

Traitement des données de sécurité des produits: Nous stockons et évaluons toutes les données personnelles dans le cadre de nos obligations légales en tant que fabricant d'un dispositif médical et transmettons ces données personnelles (si possible après pseudonymisation) aux autorités compétentes, aux organismes notifiés ou à d'autres responsables des données ayant des obligations de surveillance. En outre, nous stockerons et transférerons des données personnelles relatives aux dispositifs médicaux et/ou aux médicaments si nous recevons des communications de votre part en tant que rapporteur de ces informations, de votre patient ou d'un tiers (par exemple, nos distributeurs ou importateurs des **outils myoncare** dans votre pays) qui doivent être signalées au fabricant du produit afin que celui-ci puisse se conformer à ses obligations légales en matière de sécurité du produit.

Règles du RGPD

La base juridique du traitement des données à caractère personnel pour l'exécution d'obligations légales en tant que fabricant de dispositifs médicaux ou de médicaments est l'art. 6 par. 1 lit. c, art. 9 par. 2 lit. i le RGPD en liaison avec les obligations de surveillance post-commercialisation en vertu de la législation sur les dispositifs médicaux et de la directive sur les dispositifs médicaux (réglementée à partir du 26 mai 2021 au chapitre VII du nouveau règlement sur les dispositifs médicaux (UE) 2017/745) et/ou de la législation sur les médicaments.

QUELLE EST LA TECHNOLOGIE UTILISÉE PAR LE PORTAIL MYONCARE ET L'APPLICATION MYONCARE ?

Le **portail myoncare** fonctionne comme un outil Web pour lequel vous avez besoin d'une connexion Internet fonctionnelle et de toute version actuelle du navigateur Internet Chrome, Firefox ou Safari.

Service d' E-mail

Nous utilisons Brevo (fourni par Sendinblue GmbH, situé à Köpenicker Straße 126, 10179 Berlin) et Sendgrid (fourni par Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, États-Unis). Ces services d'e-mail peuvent être utilisés pour organiser l'envoi des e-mails. Sendgrid est utilisé pour envoyer des e-mails de confirmation, des confirmations de transaction et des e-

mails contenant des informations importantes relatives aux demandes. Les données que vous saisissez dans le but de recevoir des e-mails sont stockées sur les serveurs de Sendgrid. Lorsque nous envoyons des e-mails en votre nom via SendGrid, nous utilisons une connexion sécurisée SSL.

La communication par e-mail est utilisée pour les tâches suivantes :

- Se connecter pour la première fois à l'application web ;
- Workflow de réinitialisation du mot de passe de l'application web ;
- Créez un compte pour l'application patient ;
- Flux de travail de réinitialisation du mot de passe de l'application patient ;
- Génération et envoi d'un rapport ;
-Remplacer les notifications push par des emails pour PWA (Progressive Web App) dans les cas suivants :
(i) si un plan de soins prend fin dans la journée ;
(ii) si un médicament a été assigné ;
(iii) si la politique de confidentialité a été mise à jour ;
(iv) lors de l'envoi d'un rendez-vous aux patients et aux médecins, notamment pour le type de rendez-vous « appel vidéo »;
(v) toutes les informations relatives à un **CareTask** ou si un **Professionnel de la santé** a assigné une **CareTask**.

Brevo (Politique de confidentialité) :
Politique de confidentialité - Protection des données personnelles | Brevo

SendGrid (Politique de confidentialité) :
SendGrid (politique de confidentialité) : https://SendGrid.com/resource/general-data-protection-regulation-2/

Visible

Il s'agit d'un outil d'analyse Web open source. Matomo (fourni par InnoCraft Ltd., Nouvelle-Zélande) ne transmet pas de données à des serveurs hors du contrôle d'ONCARE. Matomo est initialement désactivé lorsque vous utilisez nos services. Ce n'est que si vous êtes d'accord que votre comportement d'utilisateur sera enregistré de manière anonyme. S'il est désactivé, un « cookie persistant » sera stocké, si les paramètres de votre navigateur le permettent. Ce cookie signale à Matomo que vous ne souhaitez pas que votre navigateur soit enregistré.

Les informations d'utilisation collectées par le cookie sont transmises à nos serveurs et y sont stockées afin que nous puissions analyser le comportement des utilisateurs.
Les informations générées par le cookie concernant votre utilisation sont les suivantes :
-Rôle;
- Géolocalisation de l'utilisateur ;
-Navigateur;
- Système d'exploitation de l'utilisateur ;
-Adresse IP;
- Sites visités via web / PWA (pour plus d'informations, consultez la section sur les PWA dans cette **Politique de confidentialité**);
- les boutons sur lesquels l'utilisateur clique dans le **Portail myoncare**, dans l' **application myoncare** et dans le **myoncare PWA**
temps pendant lequel l'utilisateur a utilisé le contenu.
Les informations générées par le cookie ne seront pas transmises à des tiers.

Vous pouvez refuser l'utilisation des cookies en sélectionnant les paramètres appropriés dans votre navigateur. Cependant, veuillez noter que vous ne pourrez peut-être pas utiliser toutes les fonctionnalités dans ce cas. Pour plus d'informations, consultez : https://matomo.org/privacy-policy/ .

La base juridique du traitement des données personnelles des utilisateurs est l'art. 6 par. 1 phrase 1 lit. a RGPD. Le traitement des données personnelles des utilisateurs nous permet d'analyser le comportement d'utilisation. En évaluant les données obtenues, nous sommes en mesure de compiler des informations sur l'utilisation des différents composants de nos services. Cela nous aide à améliorer continuellement nos services et leur convivialité.

Nous traitons et stockons les données personnelles uniquement pendant la durée nécessaire à la réalisation de l'objectif visé.

TRANSFERT SÉCURISÉ DES DONNÉES PERSONNELLES

Nous utilisons des mesures de sécurité techniques et organisationnelles appropriées pour protéger de manière optimale les données personnelles que nous stockons contre la manipulation accidentelle ou intentionnelle, la perte, la destruction ou l'accès par des personnes non autorisées. Les niveaux de sécurité sont constamment révisés en collaboration avec des experts en sécurité et adaptés aux nouvelles normes de sécurité.

L'échange de données depuis et vers le portail ainsi que depuis et vers l'application est crypté. Nous proposons SSL comme protocole de cryptage pour une transmission sécurisée des données. L'échange de données est également crypté et s'effectue à l'aide de pseudo-clés.

TRANSFERTS DE DONNÉES / DIVULGATION À DES TIERS

Nous ne transmettrons vos données personnelles à des tiers que dans le cadre des dispositions légales ou sur la base de votre consentement. Dans tous les autres cas, les informations ne seront pas divulguées à des tiers, sauf si nous y sommes contraints en raison de dispositions légales impératives (divulgation à des organismes externes, y compris les autorités de surveillance ou d'application de la loi).

Nous ne partagerons des informations et des données vous concernant que si elles sont exigées par l'État ou la loi fédérale des États-Unis ; cela inclut les demandes du ministère de la Santé et des Services sociaux si l'agence souhaite vérifier la conformité avec la loi fédérale des États-Unis.

Toute transmission de données personnelles est cryptée lors de la transmission.

Les informations sur la manière dont nous traitons les données personnelles (de santé) de vos patients qui utilisent l' **application myoncare** sont résumées dans une **politique de confidentialité** distincte pour **l'application myoncare**. Vous pouvez trouver cette **politique de confidentialité pour les patients** ici. Veuillez également lire cette **politique de confidentialité des patients** soigneusement. Pour le traitement de certaines données des patients, vous êtes le responsable du traitement des données et vous êtes responsable du respect de la protection des données (par exemple, la transmission des données de traitement au patient).

INFORMATIONS GÉNÉRALES SUR LE CONSENTEMENT

Votre consentement constitue également un consentement au traitement des données en vertu de la loi sur la protection des données. Avant d'accorder votre consentement, nous vous informerons de la finalité du traitement des données et de votre droit d'opposition.

Règles du RGPD

Si le consentement concerne également le traitement de catégories particulières de données à caractère personnel, le **portail myoncare** vous en informera expressément dans le cadre de la procédure de consentement. Traitement de catégories particulières de données à caractère personnel conformément à l'art. 9 par. 1 Le RGPD ne peut avoir lieu que si cela est nécessaire en raison de dispositions légales et qu'il n'y a aucune raison de supposer que vos intérêts légitimes s'opposent au traitement de ces données à caractère personnel ou que vous avez donné votre consentement au traitement de ces données à caractère personnel conformément à l'art. 9 para 2 du RGPD.
Pour le traitement des données pour lequel votre consentement est requis (comme expliqué dans la présente **politique de confidentialité)**, le consentement sera obtenu dans le cadre du processus d'inscription. Une fois l'inscription réussie, les consentements peuvent être gérés dans les paramètres du compte du **Portail myoncare.** En outre, ONCARE vous demandera d'accepter un accord de traitement des données pour les données traitées par ONCARE sous votre responsabilité en tant que responsable du traitement des données.

DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Dans notre organisation, nous veillons à ce que seules les personnes qui sont obligées de le faire afin de remplir leurs obligations contractuelles et légales soient autorisées à traiter des données personnelles.

Dans certains cas, des prestataires de services assistent nos départements spécialisés dans l'accomplissement de leurs tâches. Les contrats de protection des données nécessaires ont été conclus avec tous les prestataires de services qui sont des sous-traitants (au sens du RGPD) pour les informations de santé / données personnelles. Ces fournisseurs de services sont Google (Google

Firebase), fournisseurs de stockage cloud et de services d'assistance.
Google Firebase est une « base de données NoSQL » qui permet la synchronisation entre le **portail myoncare** et **l'application myoncare** de votre patient. NoSQL définit un mécanisme de stockage des données qui n'est pas seulement modélisé dans des relations tabulaires en permettant une mise à l'échelle « horizontale » plus facile par rapport aux systèmes de gestion de bases de données tabulaires/relationnelles dans un cluster de machines.

À cet effet, une pseudo-clé du **portail myoncare** et de **l'application myoncare** est stockée dans Google Firebase avec le careplan correspondant. Le transfert de données est pseudonymisé pour ONCARE et ses prestataires de services, ce qui signifie qu'ONCARE et ses prestataires de services ne peuvent pas établir de relation avec vous en tant que personne concernée. Pour ce faire, les données sont cryptées pendant le transfert et utilisent des pseudo-clés pour suivre ces transferts au lieu d'identifiants personnels tels que des noms ou des adresses e-mail. La réidentification a lieu dès que les données personnelles ont atteint le compte du patient dans **l'application myoncare** ou dans votre compte dans le **portail myoncare** après vérification par des tokens spécifiques.

Nos prestataires de stockage dans le cloud offrent un stockage cloud dans lequel est stocké le gestionnaire Firebase, qui gère les URL Firebase pour le **portail myoncare**. De plus, ces prestataires de services fournissent le domaine de serveur isolé du **portail myoncare**, dans lequel vos données personnelles ainsi que celles de votre patient sont stockées. Il héberge également le service de gestion de vidéos et de fichiers de myoncare, qui permet des vidéoconférences cryptées et l'échange de données entre vous et votre patient. L'accès à vos données personnelles par vous et votre patient est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées pendant le transfert et pseudonymisées pour ONCARE et ses prestataires de services pendant le transfert et au repos. Les prestataires de services d'ONCARE n'ont à aucun moment accès à ces données personnelles.

En outre, nous faisons appel à des prestataires de services pour traiter les demandes de service (prestataires de services d'assistance) concernant l'utilisation du compte, par exemple si vous avez oublié votre mot de passe, si vous souhaitez modifier votre adresse e-mail enregistrée, etc. Les accords de traitement des commandes nécessaires ont été conclus avec ces prestataires de services ; De plus, les employés chargés du traitement des demandes de service ont été formés en conséquence. À la réception de votre demande de service, un numéro de billet lui sera attribué.
S'il s'agit d'une demande de service concernant l'utilisation de votre compte, les informations pertinentes que vous nous avez fournies lors de la prise de contact seront transmises à l'un des employés autorisés du service externe. Ils vous contacteront ensuite.
Dans le cas contraire, elles resteront traitées par du personnel Oncare spécialement agréé, comme décrit dans la section « TRAITEMENT DES DONNÉES OPÉRATIONNELLES ».

Par l'intermédiaire de nos prestataires de services d'assistance, nous utilisons l'outil RepairCode, également connu sous le nom de Digital Twin Code, qui est une plateforme d'expérience client pour gérer les commentaires externes avec la possibilité de créer des tickets d'assistance. Vous trouverez ici la Politique de confidentialité: https://app.repaircode.de/?main=main-client – Legal/privacy.

Enfin, nous affichons du contenu provenant d'Instagram (fournisseur : Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlande), tel que des images, des vidéos ou des publications. Si vous cliquez sur une publication Instagram liée, vous serez redirigé vers Instagram. Au cours de ce processus, Instagram peut définir des cookies et traiter les données des utilisateurs.
Lorsque vous visitez une page contenant une publication Instagram liée, votre navigateur peut établir automatiquement une connexion aux serveurs d'Instagram. Instagram reçoit ainsi l'information que vous avez visité le site web, même si vous n'avez pas de compte Instagram ou si vous n'êtes pas connecté. Si vous êtes connecté, Instagram peut associer la visite à votre compte utilisateur.
Politique de confidentialité:
https://privacycenter.instagram.com/policy

TRANSFERT DE DONNÉES PERSONNELLES VERS DES PAYS TIERS

Pour fournir nos services, nous pouvons faire appel à des prestataires de services situés en dehors de l'Union européenne (pays tiers). Si les données sont transférées vers un pays tiers où le niveau de protection des données personnelles est jugé insuffisant, nous veillons à ce que des mesures appropriées soient prises conformément au droit national et européen. Si nécessaire, cela inclut la mise en œuvre de clauses contractuelles types entre les parties au traitement.

Les données personnelles collectées par le **portail myoncare** ou **l'application myoncare** ne sont pas stockées dans app stores.
Les données personnelles ne seront transférées vers des pays tiers (en dehors de l'Union européenne ou de l'Espace économique européen) que si cela est nécessaire à l'exécution de l'obligation contractuelle, si la loi l'exige ou si vous nous avez donné votre consentement.

La synchronisation du **portail myoncare** avec **l'application myoncare** se déroule à l'aide de Google Firebase. Les serveurs Google Firebase sont hébergés dans l'Union européenne. Néanmoins, conformément aux conditions générales de Google Firebase, un transfert temporaire de données vers des pays dans lesquels Google et ses fournisseurs de services associés ont des succursales est possible ; pour certains services Google Firebase, les données ne sont transférées aux États-Unis qu'aux États-Unis, sauf si le traitement a lieu dans l'Union européenne ou l'Espace économique européen. L'accès non autorisé à vos données est empêché par le chiffrement de bout en bout et les jetons d'accès sécurisés. Nos serveurs sont hébergés en Allemagne. À des fins d'analyse, les e-mails envoyés avec SendGrid contiennent ce que l'on appelle un « pixel de suivi » qui se connecte aux serveurs de Sendgrid lors de l'ouverture de l'e-mail. Cela peut être utilisé pour déterminer si un e-mail a été ouvert.

Nous intégrons le contenu d'Instagram, fourni par Meta Platforms Ireland Ltd. Si vous cliquez sur une publication Instagram liée, il est possible que des données personnelles (par exemple, l'adresse IP, les informations du navigateur, les interactions) soient transmises à Meta Platforms Inc. aux États-Unis ou dans d'autres pays tiers. Meta est certifié dans le cadre de la réglementation UE-États-Unis. Data Privacy Framework (DPF), qui reconnaît un niveau adéquat de protection des données pour les transferts vers les États-Unis. Toutefois, les données peuvent également être transférées vers des pays pour lesquels il n'existe pas de décision d'adéquation de la Commission européenne. Dans de tels cas, des mesures de protection supplémentaires peuvent être nécessaires, bien que leur efficacité ne puisse pas toujours être entièrement garantie.

Règles du RGPD

Le traitement des données est basé sur votre consentement (art. 6 par. 1 lit. a du RGPD. Vous pouvez révoquer ce consentement à tout moment. La licéité des traitements de données qui ont déjà eu lieu n'est pas affectée par la révocation.

Veuillez noter que vos données sont généralement transmises par nos soins à un serveur SendGrid aux États-Unis et y sont stockées. Nous avons conclu un contrat avec Sendgrid qui contient les clauses contractuelles types de l'UE. Cela garantit un niveau de protection comparable à celui de l'UE.

Pour traiter les données d'activité, des interfaces avec les services Google Cloud (dans le cas de GoogleFit) ou avec AppleHealth ou Withings sont utilisées au sein de l'appareil mobile de **l'utilisateur de l'application**. **Outils myoncare** utilisent ces interfaces, qui sont fournies par Google, Apple et Withings, pour demander des données d'activité à des applications de santé connectées. L'enquête envoyée par **myoncare tools** ne contient aucune donnée personnelle. Les données personnelles sont mises à la disposition des **outils myoncare** via ces interfaces.

DURÉE DE CONSERVATION DES DONNÉES PERSONNELLES CONFORMÉMENT AU RGPD

Nous conserverons vos données personnelles aussi longtemps qu'elles seront nécessaires aux fins pour lesquelles elles sont traitées. Veuillez noter que de nombreuses périodes de conservation nécessitent le stockage continu des données personnelles. Cela s'applique en particulier aux obligations de conservation en vertu du droit commercial ou fiscal.

Veuillez noter qu'ONCARE est également soumis à des obligations de conservation, qui sont convenues contractuellement avec vous sur la base des dispositions légales. De plus, en raison de la classification et, le cas échéant, de votre utilisation du **portail myoncare** et de **l'application MyonCare** en tant que dispositif médical, certaines durées de conservation s'appliquent au portail, qui résultent de la loi sur les dispositifs médicaux. S'il n'y a pas d'autres obligations de conservation, les données personnelles seront systématiquement supprimées dès que l'objectif aura été atteint.

En outre, nous pouvons conserver des données personnelles si vous nous avez donné votre consentement pour le faire ou si un litige survient et que nous utilisons des preuves dans les délais de prescription légaux, qui peuvent aller jusqu'à 30 ans; Le délai de prescription normal est de trois ans.

TRANSFERTS DE DONNÉES PERSONNELLES

Diverses données à caractère personnel sont nécessaires à l'établissement, à l'exécution et à la résiliation de la relation contractuelle ainsi qu'à l'exécution des obligations contractuelles et légales qui y sont liées. Il en va de même pour l'utilisation de notre **application myoncare** et les différentes fonctions qu'il offre.

DÉCISIONS AUTOMATISÉES (CONFORMÉMENT AU RGPD) DANS DES CAS INDIVIDUELS

Nous n'utilisons pas de traitement purement automatisé pour prendre des décisions.

VOS DROITS EN TANT QUE PERSONNE CONCERNÉE EN VERTU DU RGPD)

Nous souhaitons vous informer de vos droits en tant que personne concernée. Ces droits sont énoncés aux articles 15 à 22 du RGPD et comprennent :

Droit d'accès (art. 15 du RGPD) : Vous avez le droit de demander des informations sur la manière dont vos données personnelles sont traitées, y compris des informations sur les finalités du traitement, les destinataires, la durée de conservation et vos droits de rectification, d'effacement et d'opposition. Vous avez également le droit de recevoir une copie de toutes les données personnelles que nous détenons à votre sujet.

Droit à l'effacement / droit à l'oubli (art. 17 du RGPD) : Vous pouvez nous demander de supprimer vos données personnelles collectées et traitées par nos soins dans les meilleurs délais. Dans ce cas, nous vous demanderons de supprimer le **portail myoncare** depuis votre ordinateur. Veuillez toutefois noter que nous ne pouvons supprimer vos données personnelles qu'après l'expiration des délais de conservation légaux.

Droit de rectification (Art. 16 du RGPD) : Vous pouvez nous demander de mettre à jour ou de corriger des données personnelles inexactes vous concernant ou de compléter des données personnelles incomplètes.

Droit à la portabilité des données (Art. 20 du RGPD) : En principe, vous pouvez demander que nous vous fournissions les données à caractère personnel que vous nous avez fournies et qui sont traitées automatiquement sur la base de votre consentement ou de l'exécution d'un contrat avec vous sous une forme lisible par machine afin qu'elles puissent être « portées » à un prestataire de services de remplacement.

Droit à la limitation du traitement des données (Art. 18 du RGPD) : Vous avez le droit de demander la limitation du traitement de vos données à caractère personnel si l'exactitude des données est contestée, si le traitement est illégal, si les données sont nécessaires à des actions en justice ou si une opposition au traitement est en cours d'examen.

Droit d'opposition au traitement des données (Art. 21 du RGPD) : Vous avez le droit de vous opposer à l'utilisation de vos données personnelles et de retirer votre consentement à tout moment si nous traitons vos données personnelles sur la base de votre consentement. Nous continuerons à fournir nos services s'ils ne dépendent pas du retrait du consentement.

Pour exercer ces droits, veuillez nous contacter à l'adresse suivante : privacy@myoncare.com. L'opposition et la révocation du consentement doivent être déclarées sous forme de texte à privacy@myoncare.com.
Nous vous demanderons de fournir une preuve suffisante de votre identité pour nous assurer que vos droits sont protégés et que vos données personnelles ne seront divulguées qu'à vous et non à des tiers.

Veuillez également nous contacter à tout moment à privacy@myoncare.com si vous avez des questions sur le traitement des données dans notre entreprise ou si vous souhaitez retirer votre consentement. Vous avez également le droit de contacter l'autorité de contrôle compétente en matière de protection des données.

DÉPOSER UNE PLAINTE

Si vous estimez que votre vie privée a été violée par ONCARE, vous pouvez déposer une plainte auprès de nous et des États-Unis. Département de la Santé et des Services sociaux à Washington, D.C. Il n'y a aucun inconvénient pour vous à déposer une plainte. Pour déposer une plainte ou recevoir de plus amples renseignements, veuillez utiliser les options de contact suivantes :
Téléphone : +49 (0) 89 4445 1156

E-mail : priacy@myoncare.com
Adresse : Balanstraße 71a
81541 Munich, Allemagne
Objet : Plainte
Vous pouvez déposer une plainte auprès des États-Unis. Ministère de la Santé et des Services sociaux, en écrivant une lettre au 200 Independence Avenue, S.W., Washington, D.C. 20201 ou en composant le 1-800-368-1019 (sans frais) ou le 1-800-537-7697 (DTT) ou en déposant une plainte en ligne à https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (CONFORMÉMENT AU RGPD)

Notre délégué à la protection des données est à votre disposition pour répondre à toutes les questions sur la protection des données privacy@myoncare.com .

MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Nous nous réservons expressément le droit de modifier cette **politique de confidentialité** à l'avenir, à notre seule discrétion. Des modifications ou des ajouts peuvent être nécessaires, par exemple, pour répondre à des exigences légales, pour se conformer à l'évolution technique et économique ou pour répondre aux intérêts de **l'application** ou **des utilisateurs du portail**.

Des modifications sont possibles à tout moment et vous seront communiquées de manière appropriée et dans un délai raisonnable avant qu'elles n'entrent en vigueur (par exemple, en publiant une **Politique de confidentialité** lors de la connexion ou en prévenant à l'avance des modifications importantes).

En cas de questions d'interprétation ou de litiges, seule la version allemande de la politique de confidentialité est contraignante et fait foi.

ONCARE GmbH.

Adresse postale

Balanstraße 71a

81541 Munich, Allemagne

L | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Coordonnées du délégué à la protection des données
privacy@myoncare.com

Dernière mise à jour le 20 Février 2025

* * * *