POLITIQUE DE CONFIDENTIALITÉ POUR L'EUROPE

Bienvenue dans myoncare, le portail de santé numérique et l'application mobile (« **application** ») destinés à offrir des soins efficaces et orientés vers les besoins des patients et à soutenir les programmes de santé professionnels.

Pour nous, chez Oncare GmbH (ci-après «**ONCARE"** ou «**nous**", **"Nous**", "**notre**"), la protection de votre vie privée et de toutes les données personnelles vous concernant lors de l'utilisation du **appli** est d'une grande importance. Nous sommes conscients de la responsabilité qui découle de votre confiance dans la mise à disposition et le stockage de vos données personnelles (de santé) dans l'application 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 à la législation applicable en matière de protection des données personnelles, en particulier au Règlement général sur la protection des données de l'UE («**RGPD »)** et les lois spécifiques à chaque pays qui s'appliquent à nous. Cette politique de confidentialité explique pourquoi et comment **ONCARE** Traite vos données personnelles (de santé) que nous collectons auprès de vous ou que vous nous fournissez lorsque vous décidez d'utiliser l'application myoncare. En particulier, vous trouverez une description des données à caractère personnel que nous collectons et traitons, ainsi que la finalité et la base sur lesquelles nous traitons les données à caractère personnel et les droits dont vous disposez.

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

Conformément aux conditions d'utilisation, notre offre s'adresse uniquement aux personnes âgées 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.

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 (Patient et/ou Employé).

"**blockchain**" est une autre base de données décentralisée dans le système myoncare qui stocke les données correspondantes de l'application.

« **Société** » désigne votre employeur, si vous et votre employeur utilisez les outils myoncare dans le cadre du programme de santé professionnel de l'employeur.

"**Fournisseur de services de données**» désigne tout agent engagé et mandaté par la Société pour collecter, examiner et interpréter les données pseudonymisées ou anonymisées des employés dans les programmes de gestion de la santé au travail sur la base d'un contrat de service distinct avec la Société (par exemple, analyste de données, services généraux de prévention de la santé, services d'évaluation des données, etc.), qui sont fournies aux employés par une fiche d'information distincte.

"**Fournisseur de soins de santé**» désigne votre médecin, clinique, établissement de santé ou autre professionnel de la santé agissant seul ou au nom de votre médecin, clinique ou établissement de santé.

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

"**L'application myoncare**» désigne l'application mobile myoncare à l'usage des patients ou des salariés qui souhaitent utiliser les services proposés par ONCARE.

"**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 utilisateurs de l'application.

« **Outils myoncare** » désigne à la fois 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.

"**Services de myoncare**» désigne les services, fonctionnalités et autres offres qui sont ou peuvent 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 tout prestataire de soins de santé, entreprise ou prestataire de services de données qui utilise le portail web myoncare.

"**politique de confidentialité**» désigne la présente déclaration qui vous est remise en tant que patient et utilisateur de l'application 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 de l'application myoncare.

TRAITEMENT DES DONNÉES (OPÉRATIONNELLES)

Oncare GmbH, une société enregistrée auprès du tribunal local de Munich sous le numéro de registre 219909 avec ses bureaux situés à Balanstrasse 71a, 81543 Munich, Allemagne, propose et exploite l'application mobile **myoncare** donnant 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 de l' **application myoncare**.

QU'EST-CE QU'UNE DONNÉE PERSONNELLE

"**données personnelles**» désigne toute information permettant d'identifier une personne physique. Il s'agit notamment de votre nom, de votre date de naissance, de votre adresse, de votre numéro de téléphone, de votre adresse e-mail et de votre adresse IP.

"**Données de santé**» désigne les données à caractère personnel relatives à la santé physique et 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, données «**pseudonymisées** 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.

L'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 :
- Discutez avec **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 dans notre **application myoncare**, en nous contactant au sujet de problèmes avec l'application ou en interagissant avec nous dans le but d'utiliser l'application**.**

Données de traitement: Vous ou votre prestataire de soins de santé nous fournissez vos données personnelles, telles que le nom, l'âge, la taille, le poids, l'indication, les symptômes de la maladie et d'autres informations liées à votre traitement (par exemple dans un plan de soins). Les informations relatives à votre traitement comprennent, sans s'y limiter: les renseignements sur les médicaments pris, les réponses aux questionnaires comprenant des informations relatives à la maladie ou à l'état, les diagnostics et les thérapies fournis par votre **fournisseur de soins de santé,** les tâches planifiées et terminées.

Données d'activité: Données à caractère personnel que nous traitons si vous vous connectez à l'**application myoncare** à une application de santé (par exemple GoogleFit, AppleHealth, Withings). Vos données d'activité seront transférées à vos **prestataires de soins de santé** affiliés comme **utilisateurs du portail.**

Données de recherche commerciales et non commerciales :
Nous traitons vos données personnelles sous forme anonymisée/pseudonymisée afin d'analyser et de 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 données personnelles peuvent être traitées par des dispositifs médicaux ou des entreprises pharmaceutiques à des fins de sécurité juridique ou de vigilance.

Données de remboursement : Données personnelles nécessaires au processus de remboursement entre votre prestataire de soins de santé et votre fournisseur d'assurance maladie.

Données de gestion de la santé au travail : Données personnelles ou agrégées collectées dans le cadre de projets et de questionnaires spécifiques à la demande de votre **entreprise** (soit directement, soit par l'intermédiaire d'un fournisseur de services de données contracté par votre entreprise). Les données peuvent concerner certaines informations de santé, votre opinion sur votre bien-être personnel, votre opinion en tant que collaborateur sur une situation interne ou externe particulière, ou des données sur les soins ou la santé en général.

TECHNOLOGIE BLOCKCHAIN

Technologie Blockchain ("**blockchain**") (brevet européen n° 4 002 787) est un service facultatif qui n'est pas obligatoire. C'est votre **fournisseur de santé** qui décide 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. 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. Dans ce cas, le bloc ne peut plus être synchronisé avec les autres. Ce procédé technique empêche les personnes non autorisées de manipuler le contenu de la chaîne blockchain. Si tous les nœuds (nœuds du réseau) tentent de synchroniser leurs copies, il est détecté qu'une copie a été modifiée et le réseau considère que ce nœud est défectueux.

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** privées 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** privées dépend de l'autorisation pour devenir un utilisateur. Cette structure permet de profiter de la sécurité et de l'immuabilité de la technologie blockchain tout en étant conforme à la protection des données et en respectant notamment la réglementation du Règlement Général sur la Protection des Données (RGPD). Les enregistrements privés de la blockchain peuvent être modifiés, altérés ou supprimés ; 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. Les enregistrements des blockchains privées peuvent être modifiés, outrepassés ou supprimés ; la suppression signifie dans ce contexte d'effacer la référence à l'identifiant unique universel (UUID) dans la base de données du client.

Type de données stockées et traitées dans la blockchain:

- Institutions/Leistungserbinger UUID
- Patients-UUID
- Asset-UUID
- Code de hachage des données de CareTask et de fichiers.

(UUID : Identifiant unique universel).

Les données stockées dans la **blockchain** sont pseudo-anonymisées.

Notre **blockchain** est conçue pour garantir la confidentialité des données en termes d'intégrité des données, de profil du patient, de fichiers et des**CareTasks** et des médicaments assignées. Pour communiquer avec la **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 du **fournisseur de soins 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 du **fournisseur de santé**, accessible uniquement au patient.

Lors de la vérification du consentement à la protection des données, dans le cas où le **fournisseur de santé** veut communiquer avec le patient, le système vérifie si le patient a donné son consentement à la politique de confidentialité du **fournisseur de soins de santé**. 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 la **blockchain**. Chaque fois qu'il 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 façon, 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.

Base juridique du traitement des données : Traitement des données par ONCARE pour le **fournisseur de soins de santé** est effectué sur la base de l'art. 28 du RGPD (Accord sur le traitement des données).

TRAITEMENT DES DONNÉES OPÉRATIONNELLES

Applicable à tous les utilisateurs de l'application

Vous pouvez nous fournir certaines informations personnelles lorsque vous nous contactez pour comprendre les fonctionnalités et l'utilisation de **l'application myoncare**, en cas de demande de service ou dans le cas d'offres d'assistance initiées par nos soins (par téléphone).

Personnel de service
Au nom du responsable du traitement (par exemple, un prestataire de soins de santé), nous vous proposons une assistance téléphonique (appels sortants) pour remplir des questionnaires afin d'optimiser votre prise en charge numérique des patients. Si vous choisissez de ne pas utiliser ce service, vous êtes libre de refuser et de vous opposer à l'assistance téléphonique.

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

- Les données personnelles que vous avez fournies à votre **fournisseur de soins de santé** via notre **appli** (par exemple, nom, date de naissance, photo de profil, coordonnées).

- Les données de santé que vous avez fournies à votre **fournisseur de soins de santé**le **fournisseur de services de données** ou l' **entreprise**via notre **application myoncare** (p. ex., renseignements sur les médicaments pris, réponses à des questionnaires contenant des renseignements sur la maladie ou l'affection, diagnostics et traitements par des professionnels de la santé, tâches planifiées et terminées).

Les employés autorisés d'ONCARE qui peuvent accéder à la base de données de votre **fournisseur de soins de santé**, de votre **prestataire de services de données** ou de votre **entreprise** dans le but de traiter une demande de service ou d'effectuer un appel sortant, sont contractuellement tenus de garder toutes les données personnelles strictement confidentielles.

Notifications push et 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 de vous tenir informé de vos tâches et des mises à jour importantes pour mieux soutenir votre santé.
- 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.

Lorsque l' **application myoncare** est téléchargée, les informations nécessaires sont transmises au fournisseur de l'App Store. Nous n'avons aucun contrôle sur cette collecte de données et n'en sommes pas responsables. Nous traitons les données à caractère personnel qui nous sont fournies par le fournisseur de l'App Store dans le cadre de notre relation contractuelle dans le but de développer davantage notre **Applications myoncare** et services.

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: votre nom, adresse e-mail, numéro de téléphone, date de naissance, date d'inscription, pseudo-clés générées par l'application; tokens d'appareil permettant d'identifier votre appareil, pseudo-numéro d'identification, adresse IP, le type et la version du système d'exploitation utilisé par votre appareil.

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 de plus amples informations 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.

Finalités du traitement des données opérationnelles: Nous utilisons les données opérationnelles pour maintenir les fonctionnalités de l' **application myoncare** et pour vous contacter directement si nécessaire ou si vous nous contactez (par exemple en cas de modifications des conditions générales, d'assistance nécessaire, de problèmes techniques, d'aide pour remplir des questionnaires, etc.).

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 l' **application 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 visiter https://ipapi.com/privacy/ et

TRAITEMENT DES DONNÉES (OPÉRATIONNELLES)

Applicable aux utilisateurs de l'application qui utilisent l'application avec leur fournisseur de soins de santé

Lors de l'utilisation de l' **application myoncare**, votre **fournisseur de soins de santé** peut saisir vos données personnelles sur le **portail myoncare** afin de démarrer les **services myoncare** (ex : créer votre dossier patient, fournir une tâche individuelle, rappeler la prise de médicaments, etc.). De plus, vous et votre **fournisseur de soins de santé** peut télécharger des documents et des fichiers dans l' **application myoncare** et le **portail myoncare** et les partager les uns avec les autres. Votre **fournisseur de soins de santé** peut télécharger une **politique de confidentialité** pour votre information et définir d'autres exigences en matière de consentement pour vous en tant que patient pour lesquelles votre consentement doit être donné. Les fichiers sont stockés dans une base de données cloud en Allemagne. Votre **fournisseur de soins de santé** peut autoriser le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de son institution ou avec d'autres **fournisseurs de soins de santé** à l'extérieur de son établissement (**fournisseur de soins de santé** consultation) à des fins médicales. Les autres utilisateurs du portail n'ont pas accès à ces fichiers, sauf si l'accès est fourni par votre **fournisseur de soins de santé**. De plus, votre **fournisseur de soins de santé** peut nous demander de vous aider par téléphone à remplir des questionnaires (appels sortants). Ceci est effectué uniquement sous la direction de votre **fournisseur de soins de santé** et exclusivement par les employés autorisés d'ONCARE.

Nous utiliserons et traiterons vos données conformément à ce qui est indiqué dans cette **politique de confidentialité**, dans la mesure où vous nous donnez votre consentement.

Nous traitons ces données personnelles, y compris vos données de santé, dans le cadre d'un accord et conformément aux instructions de votre **fournisseur de soins de santé** (accord de traitement des données). Aux fins du présent accord de traitement des données, le **fournisseur de soins de santé** est responsable du traitement de vos données personnelles et de vos données de santé au sens des lois applicables en matière de protection des données en tant que responsable des données, et ONCARE est le sous-traitant de ces données personnelles (de santé). Cela signifie qu'ONCARE ne traite les données personnelles que conformément aux instructions du **fournisseur de santé**. Si vous avez des questions ou des préoccupations concernant le traitement de vos données personnelles ou de vos données de santé, vous devez contacter votre **fournisseur de soins de santé** en premier lieu.

Types de données: nom, date de naissance, informations de profil, coordonnées ainsi que des données de santé, telles que des symptômes, des photos, des informations sur les médicaments pris, des réponses à des questionnaires comprenant des informations relatives à la maladie ou à l'affection, des diagnostics et des thérapies des professionnels de santé, des tâches planifiées et réalisées.

Finalités du traitement des données: Nous traitons vos données de traitement afin de pouvoir fournir nos **services myoncare** à votre **fournisseur de soins de santé** et à vous. Vos données de santé, que vous saisissez dans notre **application myoncare**, seront utilisées par votre **fournisseur de soins de santé** pour vous conseiller et vous soutenir. Nous traitons ces données personnelles dans le cadre d'un accord avec et conformément aux instructions de votre **fournisseur de soins de santé**. La transmission de ces données de traitement est pseudonymisée et cryptée. Pour exercer vos droits en tant que personne concernée, veuillez vous adresser à votre **fournisseur de soins de santé**.

Justification du traitement des données de traitement : Vos données personnelles (de traitement) seront traitées par votre **fournisseur de soins de santé** conformément aux dispositions de la **RGPD** et toutes les autres réglementations applicables en matière de protection des données. Les bases juridiques du traitement des données résultent notamment de l'art. 9 par. 2 lit. h RGPD pour les données de santé en tant que données dignes d'une protection particulière ainsi que votre consentement conformément à l'art. 6 par. 1 lit. a et 9 par. 2 lit. a RGPD. Le traitement des données par ONCARE pour votre **fournisseur de soins de santé** est également effectuée sur la base de l'art. 28 du RGPD (accord de traitement des commandes).

Votre **fournisseur de soins de santé**, en tant que responsable des données, est responsable de l'obtention de votre consentement. Même si vous pouvez utiliser l' **application myoncare** sans ce consentement, la plupart des fonctions ne fonctionneront plus (par exemple, le partage de données avec votre **fournisseur de soins de santé**). Par conséquent, le refus ou la révocation du consentement au traitement des données entraîne une restriction sévère de la fonctionnalité des services de l'application et votre **fournisseur de soins de santé** ne peut plus vous assister via l' **application myoncare**.

TRAITEMENT DES DONNÉES D'ACTIVITÉ

Seulement applicable si vous acceptez et activez le transfert de données d'activité via les outils myoncare

Outils myoncare vous offrent la possibilité de connecter l' **application myoncare** avec certaines applications de santé (par exemple AppleHealth, GoogleFit, Withings) que vous utilisez («**Application Santé**"). Afin de permettre le traitement des données d'activité, nous obtiendrons votre consentement préalable au traitement. Si la connexion est établie après que vous ayez donné votre consentement, les données d'activité collectées par l' **Application Santé** seront mis à la disposition de vos **fournisseurs de santé** dans le but de fournir des informations contextuelles supplémentaires concernant votre activité. Veuillez noter que les données d'activité ne sont pas validées par **les outils myoncare** et ne doivent pas être utilisées par votre **fournisseur de soins de santé** à des fins de diagnostic comme base pour la prise de décision médicale. Veuillez également noter que votre **prestataires de soins de santé** ne sont pas obligés de vérifier vos données d'activité et n'ont pas à vous donner de commentaires concernant vos données d'activité.
Les données d'activité sont partagées avec vos **prestataires de soins de santé** affiliés chaque fois que l'**application myoncare** est accédée. Vous pouvez révoquer votre consentement au partage des données d'activité à tout moment dans les paramètres de l' **application myoncare**. Veuillez noter que vos données d'activité ne seront plus partagées à partir de ce moment. Les données d'activité qui sont déjà été partagées ne seront pas supprimées de lu **Portail myoncare** de vos **prestataires de soins de santé** affiliés.
Le traitement des données d'activité relève de votre propre responsabilité.

Types de données : Le type et l'étendue des données transférées dépendent de votre décision et de la disponibilité de ces données dans le cadre de l' **application de santé.** 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 : Vos données d'activité seront mises à la disposition de vos **Prestataires de soins de santé** avec qui vous êtes connecté dans le but de fournir des informations supplémentaires et contextuelles concernant votre activité.

Justification du traitement : Le traitement des données d'activité relève de votre propre responsabilité.

TRAITEMENT DES DONNÉES DE SÉCURITÉ DU PRODUIT

Applicable aux utilisateurs de l'application dont le fournisseur de soins de santé utilise la variante de dispositif médical des outils myoncare

L' **application myoncare** est classée et commercialisée en tant que dispositif médical conformément à la réglementation européenne sur les dispositifs médicaux. En tant que fabricant de l'application, nous devons respecter certaines obligations légales (par exemple, surveiller le fonctionnement de l'application, évaluer les rapports d'incident qui pourraient être liés à l'utilisation de l'application, suivre les utilisateurs, etc.). De plus, l' **application myoncare**permet **à** vous et votre **fournisseur de santé** de communiquer et collecter des données personnelles concernant certains dispositifs médicaux ou médicaments utilisés dans votre traitement. 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 déclarations d'effets indésirables).

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

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

Traitement des données de sécurité du produit : 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 en relation avec des dispositifs médicaux et/ou des médicaments si nous recevons des notifications de la part de votre **fournisseur de soins de santé**, de votre part en tant que patient ou d'un tiers (par exemple, nos distributeurs ou importateurs des **outils myoncare** dans votre pays) qui doivent être signalés au fabricant du produit afin que le fabricant 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 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.

MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Applicable aux utilisateurs de l'application qui utilisent l'application avec leur fournisseur de soins de santé à des fins de remboursement

L' **application myoncare** soutient votre **fournisseur de soins de santé** en engageant des procédures standard de remboursement des coûts des services de santé qui vous sont fournis par l'intermédiaire de l' **application myoncare**. Afin de permettre le processus de remboursement, l' **application myoncare** soutient la collecte de vos données personnelles (de santé) par vos **fournisseur de soins de santé** pour la transmission de ces données à votre unité payeuse (soit son Association des médecins de l'assurance maladie obligatoire et/ou votre compagnie d'assurance maladie). Ce traitement de données n'est qu'un premier transfert de données pour le **fournisseur de soins de santé** afin d'obtenir un remboursement de votre caisse d'assurance maladie. Le type et la quantité de données personnelles traitées ne diffèrent pas des autres procédures de remboursement du **fournisseur de santé**. Votre **fournisseur de soins de santé** est le responsable des données de remboursement. ONCARE agit en tant que sous-traitant sur la base de l'accord de traitement des données conclu avec votre **fournisseur de santé**.

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

Traitement des données de remboursement: Votre **fournisseur de soins de santé** transmet vos données de traitement nécessaires au remboursement au payeur (soit son institution d'assurance maladie légale et/ou votre compagnie d'assurance maladie) et le payeur traite les données de remboursement afin de rembourser votre **fournisseur de soins de santé**.

Justification du traitement des données de remboursement: Les données de remboursement sont traitées sur la base des §§ 295, 301 SGB V, art. P, par. 2 lit. b RGPD. Le traitement des données par ONCARE pour votre **fournisseur de soins de santé** est également effectuée sur la base de l'art. 28 du RGPD (accord de traitement des commandes).

TRAITEMENT DES DONNÉES DE GESTION DE LA SANTÉ AU TRAVAIL

Applicable aux utilisateurs de l'application qui utilisent l'application avec la gestion de la santé au travail de l'entreprise

Lors de l'utilisation de l' **application myoncare** dans le cadre de la gestion de la santé au travail **de l'entreprise** , certaines données personnelles (de santé) sont transmises sous forme agrégée en tant que données pour la gestion de la santé au travail à l'**entreprise** et aux **prestataires de services de données** commandé par l'**entreprise** (par exemple, des analystes de données ou des sociétés de recherche). Ni la **Société** ni aucun **fournisseur de services de données** ne peuvent

attribuer de telles données à votre identité. ONCARE recommande de ne partager aucune donnée personnelle lors de l'utilisation des **services myoncare** dans le cadre de la gestion de la santé au travail.

Cela signifie que ONCARE et tous les **fournisseurs de services de données** ne traiteront les données que pour la gestion de la santé au travail conformément aux instructions **de l'entreprise**. Nous traitons ces données pour la gestion de la santé au travail, y compris vos données de santé, sur la base d'un accord avec votre **entreprise**et/ou un **fournisseur de services de données** et conformément à leurs instructions. Aux fins du présent Accord, l' **entreprise**ou le **fournisseur de services de données** est le responsable du traitement de vos données à des fins de gestion de la santé au travail et d'ONCARE et de tous **fournisseurs de services de données** engagés par l' **entreprise**, le cas échéant, sont les sous-traitants de ces données. Si vous avez des questions ou des préoccupations concernant le traitement de vos données pour la gestion de la santé au travail, vous devez contacter l' **entreprise** en premier lieu**.**

Finalités du traitement des données dans la gestion de la santé au travail : Nous traitons vos données pour la gestion de la santé au travail afin de pouvoir vous offrir, ainsi qu'à l' **entreprise**, nos services **myoncare**. Les données de gestion de la santé de votre entreprise, que vous saisissez dans notre **application myoncare**, seront utilisées par l' **entreprise** (soit directement, soit par l'intermédiaire d'un **fournisseur de services de données**) dans le cadre de sa gestion de la santé au travail. Nous traitons ces données pour la gestion de la santé au travail dans le cadre d'un accord avec l' **entreprise** et/ou un **fournisseur de services de données** pour sa gestion de la santé au travail. La transmission de ces données pour la gestion de la santé au travail est pseudonymisée et cryptée. Pour exercer vos droits en tant que personne concernée, veuillez vous adresser à l' **entreprise**.

Justification du traitement des données de gestion de la santé au travail : Vos données de gestion de la santé au travail seront traitées par l' **entreprise** conformément aux dispositions de la **RGPD** et toutes les autres réglementations applicables en matière de protection des données. La base juridique du traitement des données est notamment votre consentement conformément à l'art. 6 par. 1 lit. a et de l'art. 9 par. 2 lit. un RGPD ou tout autre fondement juridique applicable à l' **entreprise**. Le traitement des données par ONCARE auprès de l' **entreprise** (soit directement, soit par l'intermédiaire d'un **fournisseur de soins de santé** mandaté par votre entreprise) est également basé sur l'art. 28 du RGPD (Accord sur le traitement des données). L' **entreprise** en tant que responsable du traitement des données, est responsable de l'obtention de votre consentement si la réglementation sur la protection des données l'exige et du traitement des données à des fins de gestion de la santé au travail conformément aux lois applicables en matière de protection des données.

QUELLE EST LA TECHNOLOGIE UTILISÉE PAR L'APPLICATION MYONCARE ?

Service de courrier électronique
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 de courrier électronique 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 ;
- Remplacez les notifications push par des e-mails pour **PWA** (Progressive Web App) dans les cas suivants :
  (i) si un plan de soins se termine dans une heure;
  (ii) si un médicament a été assigné ;
  (iii) si la politique de confidentialité a été mise à jour ;

(iv) lorsqu'un rendez-vous est envoyé aux patients et aux médecins, en particulier pour le type de rendez-vous « appel vidéo » ;
(v) Toute information relative à une **CareTask** ou si un **fournisseur de 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/

Matomo
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 de l'utilisateur ;
- Géolocalisation de l'utilisateur ;
- Système d'exploitation utilisateur ;
- Temps pendant lequel l'utilisateur a utilisé le contenu ;
-Adresse IP;
- Sites visités via web / **PWA** (pour plus d'informations, consultez la section sur les PWA dans la présente Politique de confidentialité) ;
- les boutons sur lesquels l'utilisateur clique dans le **portail myoncare**, l' **application myoncare** et le **PWA myoncare**.

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 ne traitons et ne conservons les données personnelles qu'aussi longtemps que nécessaire pour atteindre 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 vers et depuis l'application est crypté. Nous utilisons TLS et SSL comme protocoles de cryptage pour le transfert sécurisé 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).

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

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 d'accorder 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, l' **application 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 la loi l'exige 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 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 de l' **application myoncare**.

DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Au sein de notre organisation, nous veillons à ce que seules les personnes autorisées à traiter les données personnelles nécessaires à l'exécution de leurs obligations contractuelles et légales. Vos données personnelles et les données de santé que vous saisissez dans notre **application myoncare** seront mis à la disposition de votre **fournisseur de soins de santé** et/ou **entreprise** soit directement, soit par l'intermédiaire d'un **fournisseur de services de données** (selon le type d'utilisation des **outils myoncare**).

Dans certains cas, **d'autres 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 **prestataires de services** sont Google (Google Firebase), des 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 de votre prestataire de soins de santé** et **l'application myoncare**. 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 cette fin, une pseudo-clé de l' **application myoncare** est stockée dans Google Firebase ainsi que le **CarePlan** correspondant. Le transfert de données est pseudonymisé pour ONCARE et ses prestataires de services, ce qui signifie qu'ONCARE et ses autres prestataires de services ne peuvent pas établir de relation avec vous en tant que personne concernée. Ceci est réalisé en cryptant les données lors du transfert entre vous et vos **prestataires de soins de santé** ou **votre entreprise** (soit directement, soit vers n'importe quel **fournisseur de services de données**) et en utilisant des pseudo-clés au lieu d'identificateurs personnels tels que le nom ou l'adresse e-mail pour suivre ces transferts. La réidentification a lieu dès que les données personnelles ont atteint le compte de votre **prestataires de soins de santé** ou **de votre entreprise** sur le **portail myoncare** ou votre compte dans l' **application myoncare**, après avoir été vérifié par des tokens spécifiques.

Nos fournisseurs de stockage en nuage proposent un stockage en nuage dans lequel le gestionnaire Firebase, qui gère les URL Firebase pour le **portail myoncare**, est stocké. De plus, ces fournisseurs de services fournissent le domaine de serveur isolé du **portail myoncare**, dans lequel vos données personnelles sont stockées. Il héberge également les services de gestion de vidéos et de fichiers de myoncare, qui permettent des vidéoconférences cryptées entre vous et votre **fournisseur de soins de santé** ainsi que l'échange de fichiers. Accès à vos données personnelles par vous et

votre **fournisseur de soins de santé** est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées pendant le transfert et au repos et pseudonymisées pour ONCARE et ses prestataires de services. 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 continueront d'être 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 notre 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 cette **application myoncare** ne sont pas stockées dans les magasins d'applications. 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 de l' **application myoncare** et le **portail myoncare** se déroule via Google Firebase. Le serveur Google Firebase est hébergé dans l'Union européenne. Toutefois, comme décrit dans les Conditions d'utilisation de Google Firebase, des transferts de données à court terme vers des pays dans lesquels Google ou ses fournisseurs de services sont situés sont possibles. 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 illégal à vos données est empêché grâce au cryptage de bout en bout et aux 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. Le cadre de confidentialité des données (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 déjà effectués n'est pas affectée par la révocation.

Veuillez noter que nous transmettons généralement vos données à un serveur SendGrid aux États-Unis et les y stockons. Nous avons conclu un contrat avec SendGrid intégrant les clauses contractuelles standards 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 dans 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 **outils myoncare** 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

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, mais sans s'y limiter, aux obligations de conservation en vertu du droit commercial ou fiscal (par exemple, le Code de commerce, la loi fiscale, etc.). De plus, votre **fournisseur de soins de santé** doit également assurer la conservation de votre dossier médical (entre 1 et 30 ans, selon le type de documents).

Veuillez noter qu'ONCARE est également soumis à des obligations de conservation convenues contractuellement avec votre **fournisseur de soins de santé** sur la base des dispositions légales. De plus, et uniquement si votre **fournisseur de soins de santé** utilise la variante de dispositif médical des **outils myoncare**, certaines périodes de conservation découlant de la Loi sur les dispositifs médicaux s'appliquent en raison de la classification de **l'application myoncare** en tant que dispositif médical. 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.

DURÉE DE CONSERVATION DES 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.

Nous avons résumé les détails pour vous sous les points ci-dessus. 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.

ACCÈS

Pour tous les appareils, quel que soit le système d'exploitation utilisé, il est nécessaire d'accorder à l'application certaines autorisations, que nous appelons « droits d'accès de base ». Selon le système d'exploitation de l'appareil que vous utilisez, il peut avoir des fonctionnalités supplémentaires qui nécessitent des autorisations supplémentaires pour que l'application fonctionne. Pour que l' **application myoncare** fonctionner sur votre appareil, l'application doit disposer de diverses autorisations pour accéder à certaines fonctions de l'appareil. Le cas échéant, nous les listerons dans l'ordre du système d'exploitation (Android ou iOS) selon les « conditions de base ».
Les droits d'accès de base (Android et iOS) sont les suivants :

Obtenir des connexions Wi-Fi
Nécessaire pour assurer la fonctionnalité du téléchargement de documents en conjonction avec les connexions Wi-Fi.

Obtenir une connexion réseau
Requise pour assurer la fonctionnalité du téléchargement de documents en conjonction avec des connexions réseau qui ne sont pas des connexions Wi-Fi.

Désactiver le verrouillage de l'écran (empêcher le mode veille)
Nécessaire pour que les vidéos qui appartiennent aux documents fournis puissent être lues directement dans l'application sans être interrompues par un verrouillage de l'écran.

Accès à tous les réseaux
L'accès à tous les réseaux est requis pour télécharger les documents.

Désactiver le mode veille
Cela est nécessaire pour que les vidéos qui appartiennent aux documents fournis puissent être lues directement dans l'application sans que la lecture ne soit interrompue par l'apparition d'une mise en veille prolongée.

Données mobiles / Accès aux données mobiles
Si l'utilisateur souhaite télécharger des documents exclusivement via Wi-Fi, il peut effectuer le réglage approprié dans le menu de l'application et désactiver l'utilisation des données mobiles. L'accès aux données mobiles est nécessaire pour garantir la fonctionnalité de désactivation des téléchargements de documents sur les données mobiles.

Accès à l'appareil photo
L'accès à la caméra est nécessaire pour scanner les QR codes ainsi que pour les consultations vidéo

Accès au microphone
L'accès au microphone est requis pour les consultations vidéo

Accéder aux fichiers et aux photos
Ceci est nécessaire pour l'échange de fichiers entre vous et les utilisateurs de votre portail connecté.

Accès par navigateur Web
Cela est nécessaire pour afficher les fichiers reçus des utilisateurs de votre portail connecté.

Nous utilisons des notifications push, qui sont des messages envoyés à votre appareil mobile en tant que service de l' **application myoncare** via des services tels que Apple Push Notification Service ou Google Cloud Messaging Service. Ces services sont des fonctionnalités standard des appareils mobiles. La politique de confidentialité du fournisseur de services régit l'accès, l'utilisation et la divulgation des renseignements personnels à la suite de votre utilisation de ces services.

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 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 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 l' **application myoncare** y compris votre UID (Unique Identification Number) de votre smartphone/téléphone portable. 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 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 de restriction 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 contacter en premier lieu votre **fournisseur de soins de santé** ou **votre entreprise** ou contactez-nous 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.

RESTRICTION D'ÂGE DE L'APPLICATION

Un âge minimum de 18 ans est requis pour utiliser l' **application myoncare**.

MODIFICATIONS DE LA POLITIQUE DE CONFIDENTIALITÉ

Nous nous réservons expressément le droit de modifier cela **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 des **utilisateurs de l' appli** ou **du portail**.
Les 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 révisée lors de la connexion ou en vous informant 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.

* * * *

États-Unis POLITIQUE DE CONFIDENTIALITÉ
Bienvenue sur myoncare, le portail de santé numérique et l'application mobile («**App**») pour des soins efficaces et à la demande aux patients et un soutien aux programmes de gestion de la santé au travail.

Cette politique de confidentialité décrit comment vos informations personnelles et médicales peuvent être utilisées et partagées, et comment vous pouvez accéder à ces informations. Veuillez lire attentivement cette politique de confidentialité. Dans cette politique de confidentialité, vous apprendrez pourquoi et comment ONCARE traite les données de santé personnelles qui nous sont fournies si vous décidez d'utiliser l'application myoncare.

Pour nous, chez Oncare GmbH (ci-après dénommée «**Oncare (ONCARE** ou «**nous**", "**nous**", "**notre**"), la protection de votre vie privée et des données personnelles vous concernant lors de l'utilisation de l'application myoncare est d'une grande pertinence et d'une grande importance. Nous sommes conscients de la responsabilité qui découle de votre confiance dans la fourniture et le stockage de vos données personnelles (de santé) dans l'application 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.

Toutes les informations que nous détenons et qui sont fournies par vos **fournisseurs 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 les États-Unis. La loi sur la portabilité et la responsabilité des assurances-maladie (**HIPAA).** 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.

L'utilisation et la divulgation de ces **PHIs** est conforme aux politiques de confidentialité applicables et lois. Pour comprendre plus en détail comment nous traitons et partageons ces **PHIs**, vous devriez lire cette **Politique de confidentialité** soigneusement**.**
Veuillez lire attentivement la politique de confidentialité pour vous assurer que vous comprenez chaque disposition. Après avoir lu la politique de confidentialité, vous avez la possibilité d'accepter la politique de confidentialité et de consentir au traitement de vos données personnelles (de santé) comme décrit dans la politique de confidentialité. Si vous donnez votre consentement, la politique de confidentialité fait partie du contrat entre vous et ONCARE. Nous garantissons les droits et obligations décrits dans la présente politique de confidentialité. Nous utilisons et traitons vos données conformément aux dispositions de la présente politique de confidentialité.

Conformément aux conditions d'utilisation, notre offre s'adresse uniquement aux personnes âgées 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.

DÉFINITIONS

« utilisateur de l'application» désigne tout utilisateur de l'Application myoncare (Patient et/ou Employé).

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

"**Entreprise**» désigne votre employeur si vous et votre employeur utilisez les outils myoncare pour la gestion de la santé au travail de l'employeur.

"**Entité visée**» désigne un régime de santé, un centre d'information sur les soins de santé ou un fournisseur de soins de santé qui soumet des informations de santé sous forme électronique dans le cadre d'une transaction relevant de la loi HIPAA.

"**Fournisseur de services de données**» désigne tout agent engagé et chargé par la Société de recueillir, d'examiner et d'interpréter les données pseudonymisées ou anonymisées des employés dans les programmes de gestion de la santé au travail sur la base d'un contrat de service distinct avec la Société (par exemple, analyste de données, services généraux de

prévention de la santé, services d'évaluation des données, etc.), qui est fourni par une fiche d'information distincte aux employés.

"**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. La 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. La RGPD s'applique également à vous en tant que citoyen américain, car Oncare est basé en Allemagne.

"**Fournisseur de soins de santé**» désigne votre médecin, clinique, établissement de santé ou autre professionnel de la santé agissant seul ou au nom de votre médecin, clinique ou établissement de santé.

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

"**Informations sur la santé**» désigne toutes les informations, y compris les informations génétiques, qu'elles soient enregistrées oralement ou sous quelque forme ou sur quelque support que ce soit, et qui
- traités ou transférés par un fournisseur 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 rapporte à la santé physique ou mentale passée, présente ou future d'une personne ou à tout état de santé lié au traitement médical de la personne, selon le cas ;
- la rémunération passée, présente ou future des soins de santé d'une personne. "**Informations de santé protégées**» ou «**PHI"** signifie les renseignements sur la santé permettant d'identifier une personne qui, selon le cas

(i) est 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**, la loi de 1996 sur la portabilité et la responsabilité de l'assurance maladie (**HIPAA)** est une loi fédérale américaine qui prévoit 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 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, qui est destiné à un usage professionnel par les utilisateurs du portail et sert d'interface entre les utilisateurs du portail et les utilisateurs de l'application.

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

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

"**ONCARE**» ou «**nous**» désigne ONCARE GmbH, dont le siège est en Allemagne.

"**Utilisateur du portail**» désigne tout prestataire de soins de santé, entreprise ou prestataire de services de données utilisant le portail web myoncare.

"**Politique de confidentialité**» désigne la présente déclaration qui vous est remise en tant que patient ou employé et utilisateur de l'application myoncare, qui décrit la manière dont nous collectons, utilisons et

stockons vos données personnelles et vous informe de vos droits.

"**L'application myonare**» désigne l'application mobile myoncare à l'usage des patients ou des employés qui souhaitent utiliser les services proposés par ONCARE.

"**Conditions d'utilisation**» désigne les conditions d'utilisation de l'application myoncare.

RESPECT DES LOIS

Oncare GmbH, une société enregistrée auprès du tribunal local de Munich sous le numéro de registre 219909 avec son bureau situés à Balanstrasse 71a, 81543 Munich, Allemagne, propose et exploite l'application mobile **myoncare** donnant accès aux **services myoncare**. La présente politique de confidentialité s'applique à toutes les données personnelles traitées par ONCARE dans le cadre de l'utilisation de **l'application myoncare**.

ONCARE est un « partenaire d'affaires » au sens de **HIPAA** qui fournit des services et des régimes de soins de santé à **des fournisseurs de soins de santé** appelés « entités couvertes » au sens de **HIPAA**; ONCARE conclut des accords de partenariat commercial avec ces entreprises couvertes. ONCARE ne traitera et ne partagera que les **PHIs** aux termes des Accords et **HIPAA**.

Nous sommes tenus par les États-Unis. Nous sommes tenus par la loi américaine de maintenir la confidentialité et la sécurité de vos informations de santé protégées.
Nous sommes tenus par la des États-Unis pour suivre 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).

Nous devons nous conformer aux obligations et au contenu décrits dans la présente politique de confidentialité et vous fournir une copie de la politique de confidentialité sur demande.

Aucune information personnelle identifiable (de santé) ne sera vendue.

Nous n'utiliserons ni ne partagerons vos informations autrement que de la manière décrite ici, à moins que vous ne nous informiez que nous sommes autorisés à le faire.

La Politique de confidentialité des États-Unis, les lois fédérales et étatiques des États-Unis peuvent imposer des restrictions supplémentaires sur le partage de vos informations de santé dans le cadre d'un traitement médical pour l'abus de drogues ou d'alcool, les maladies sexuellement transmissibles, les informations génétiques ou les programmes de traitement de la santé mentale. Si les lois applicables s'appliquent, nous obtiendrons votre consentement avant de partager ou de traiter ces données.

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

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 et les lois spécifiques à chaque pays qui nous sont applicables. 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.

"**Données personnelles**» désigne toute information permettant d'identifier une personne physique. Il s'agit notamment de votre nom, de votre date de naissance, de votre adresse, de votre numéro de téléphone, de votre adresse e-mail et de votre adresse IP.

"**Données de santé**» désigne les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de services de santé qui révèlent des informations sur son état de santé.

Les données sont considérées comme «**anonyme"** si aucune référence personnelle à la personne/utilisateur ne peut être établie. En revanche, données «**pseudonymisées**« sont des données dans lesquelles la référence personnelle ou les données personnelles 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).

L'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 la **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 le cadre de la **myoncare PWA**, voir la description ci-dessous pour plus de détails. Il s'agit des services ou spécifications suivants :

- Discutez avec les **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 la **myoncare PWA**, sauf indication contraire dans le présent article

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

Nous utilisons et partageons vos informations de santé dans le cadre d'activités commerciales habituelles qui entrent dans les catégories de traitement et de soins de santé en vertu de la loi. 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 dans notre **application myoncare**, en nous contactant au sujet de problèmes avec l'application ou en interagissant avec nous dans le but d'utiliser l'application.

Données de traitement: Vous ou votre prestataire de soins de santé saisissez des données personnelles telles que le nom, l'âge, la taille, le poids, l'indication, les symptômes de la maladie et d'autres informations en rapport avec votre traitement (par exemple dans un plan de soins) avec le soutien de l' **application myoncare**. Les renseignements relatifs à votre traitement comprennent, sans s'y limiter : des renseignements sur les médicaments pris, les réponses aux questionnaires, y compris les renseignements liés à la maladie ou à l'affection, les diagnostics et les thérapies fournis par votre **fournisseur de soins de santé** tâches planifiées et terminées).

Données d'activité: Données à caractère personnel que nous traitons si vous vous connectez à l' **application myoncare** à une application de santé (par exemple GoogleFit, AppleHealth, Withings). Vos données d'activité seront transférées à vos **prestataires de soins de santé** affiliés en tant qu'utilisateurs du portail.

Données de recherche commerciales et non commerciales: Nous traitons vos données personnelles sous forme anonymisée/pseudonymisée afin d'analyser et de 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. Par ailleurs, vos données personnelles peuvent être traitées par des entreprises de dispositifs médicaux ou pharmaceutiques pour répondre à des objectifs de sécurité juridique ou de vigilance.

Informations sur le remboursement: Données personnelles nécessaires au processus de remboursement entre votre **fournisseur de santé** myoncare et votre caisse d'assurance maladie.

Données de gestion de la santé au travail : Données personnelles ou agrégées collectées dans le cadre de projets et de questionnaires spécifiques à la demande de

l' **entreprise** (soit directement, soit par l'intermédiaire d'un **fournisseur de services de données** contracté par l' **entreprise**). Les données peuvent concerner certaines informations de santé, votre opinion sur votre bien-être personnel, votre opinion en tant que collaborateur sur une situation interne ou externe particulière, ou des données sur les soins ou la santé en général.

TECHNOLOGIE BLOCKCHAIN

Technologie blockchain ("**Blockchain**") (brevet européen n° 4 002 787) est un service facultatif qui n'est pas obligatoire. C'est votre **fournisseur de santé** qui décide d'utiliser la solution blockchain. Le **Chaîne de blocs** 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 **Chaîne de blocs** 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'un **Chaîne de blocs** ("**Blockchain privée**"), il n'autorise 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 **Chaîne de blocs** 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 détecté qu'une copie a été modifiée et le réseau considère que ce nœud est défectueux. Ce procédé technique empêche les personnes non autorisées de **manipuler** le contenu de la chaîne blockchain.

Notre **blockchain** est un **blockchain privé**. Un **blockchain privé** 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 notamment pour 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:

- Patients-UUID
- Institutions/Leistungserbinger UUID
- Asset-UUID
- Hachage de **CareTask** et données des fichiers.

(*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. 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 du **fournisseur 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 **du fournisseur 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 **fournisseur 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 la **blockchain**, et une fois que le patient a accepté la politique de confidentialité, cette interaction est stockée dans la **blockchain**. Chaque fois qu'il 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 santé**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 la **blockchain**. De cette façon, le **fournisseur de santé**atteint 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 du **fournisseur de services** est effectué sur la base de l'Art. 28 du RGPD (accord de traitement des commandes).

TRAITEMENT DES DONNÉES OPÉRATIONNELLES

Applicable à tous les utilisateurs de l'application

Vous pouvez nous fournir certaines informations personnelles lorsque vous nous contactez pour comprendre ou discuter des fonctionnalités et de l'utilisation de l'application, en cas de demande de service ou dans le cas d'offres d'assistance initiées par nos soins (par téléphone).

Personnel de service
Au nom du responsable du traitement des données (par exemple, fournisseur de soins de santé), nous vous proposons une assistance téléphonique (appels sortants) pour remplir des questionnaires afin d'optimiser votre prise en charge numérique des patients. Si vous choisissez de ne pas utiliser ce service, vous êtes libre de refuser et de vous opposer à l'assistance téléphonique.

En cas de demande de service ou d'appel sortant, les données personnelles suivantes peuvent également être consultées par les employés autorisés d'ONCARE :
- les données personnelles que vous avez fournies à votre **fournisseur de soins de santé** via notre application (par exemple, nom, date de naissance, photo de profil, coordonnées) ;
- les renseignements sur la santé que vous avez fournis à votre **fournisseur de soins de santé**le **fournisseur de services de données** ou l'entreprise via notre **application myoncare** (p. ex., renseignements sur les médicaments pris, réponses à des questionnaires comprenant des renseignements sur la maladie ou l'affection, les diagnostics et les traitements effectués par des professionnels de la santé, les tâches planifiées et terminées).

Les employés autorisés d'ONCARE qui peuvent accéder à la base de données de votre **fournisseur de soins de santé**, de votre **prestataire de services de données** ou de votre **entreprise** dans le but de traiter une demande de service, sont contractuellement tenus de garder toutes les données personnelles strictement confidentielles.

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 Webapp) 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 de vous tenir informé de vos tâches et des mises à jour importantes pour mieux soutenir votre santé.
- 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.

Lorsque l' **application myoncare** est téléchargée, les informations nécessaires sont transmises au fournisseur de l'App Store. Nous n'avons aucun contrôle sur cette collecte de données et n'en sommes pas responsables. Nous traitons les données à caractère personnel qui nous sont fournies par le fournisseur de l'App Store dans le cadre de notre relation contractuelle dans le but de développer davantage notre **Applications myoncare** et **services**.

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: votre nom, votre adresse e-mail, votre numéro de téléphone, votre date de naissance, votre date d'inscription, les pseudo-clés générées par l'application ; Tokens d'appareil permettant d'identifier votre appareil, votre pseudo-numéro d'identification, votre adresse IP, le type et la version du système d'exploitation utilisé par votre appareil.

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 de plus amples informations 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.

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. Vos données personnelles et les données de santé que vous saisissez dans notre **application myoncare** seront mises à la disposition de votre **fournisseur de soins de santé** et/ou de votre **entreprise** soit directement, soit via un **prestataire de services de données** (selon le type d'utilisation des **outils myoncare**).

Règles du RGPD: Le traitement des données de l'entreprise 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 l' **application 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 l'emplacement des utilisateurs patients. 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 leur utilisation est l'art. 6 (1) (f) du 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)
Applicable aux utilisateurs de l'application qui utilisent l'application avec leur fournisseur de soins de santé.

Lors de l'utilisation de l'application myoncare, votre **fournisseur de soins de santé** saisit vos données personnelles sur le portail myoncare afin de démarrer les services myoncare (ex: création de votre dossier patient, mise à disposition d'un plan de soins individuel, rappel de prise de médicaments, etc.). De plus, vous et votre **fournisseur de soins de santé** pouvez télécharger des documents et des fichiers sur l'**application myoncare** et le **portail myoncare** et les partager les uns avec les autres. Votre **fournisseur de soins de santé** peut télécharger une politique de confidentialité pour vos informations et définir d'autres exigences en matière de consentement pour vous en tant que patient pour lesquelles votre consentement doit être donné. Les fichiers sont stockés dans une base de données cloud en Allemagne. Votre **fournisseur de soins de santé** peut autoriser le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de son établissement ou avec d'autres **fournisseurs de soins de santé** extérieurs à son établissement (fournisseur de soins de santé consultant) à des fins médicales. Les autres utilisateurs du portail n'ont pas accès à ces fichiers, sauf si l'accès est fourni par votre **fournisseur de soins de santé**. De plus, votre **fournisseur de soins de santé** peut nous demander de vous aider par téléphone à remplir des questionnaires (appels sortants). Ceci est effectué uniquement à la demande de votre **fournisseur de soins de santé** et exclusivement par les employés autorisés d'ONCARE.

Nous utilisons et traitons vos informations de santé uniquement pour les activités opérationnelles autorisées par la loi HIPAA et d'autres lois fédérales.

Nous traitons ces données personnelles, y compris vos données de santé, dans le cadre d'un accord et conformément aux instructions de votre **fournisseur de soins de santé** (accord de traitement des données). Aux fins de cet accord, le **prestataire de soins de santé** est responsable du traitement de vos données personnelles et données de santé en vertu des lois en vigueur sur la protection des données en tant que responsable du traitement des données, et ONCARE est le sous-traitant de telles données personnelles (de santé). Cela signifie qu'ONCARE ne traite les données personnelles que conformément aux instructions du **fournisseur de santé**. Si vous avez des questions ou des préoccupations concernant le traitement de vos données personnelles ou de vos données de santé, vous devez contacter votre **fournisseur de soins de santé** en premier lieu.

TRAITEMENT DES DONNÉES D'ACTIVITÉ
Applicable uniquement si vous acceptez et activez le transfert de données d'activité via les outils myoncare

Outils myoncare vous offrent la possibilité de connecter l' **application myoncare** avec certaines applications de santé (par exemple AppleHealth, GoogleFit, Withings) que vous utilisez («**health app**"). Si la connexion est établie après que vous avez donné votre consentement, les données d'activité collectées par l'**Application Santé seront mis à la disposition de vos fournisseurs de santé** dans le but de fournir des informations contextuelles supplémentaires concernant votre activité. Afin de permettre le traitement des données d'activité, nous obtiendrons votre consentement préalable au traitement. Veuillez noter que les données d'activité ne sont pas validées par **les outils myoncare** et ne doivent pas être utilisées par votre **fournisseur de soins de santé** à des fins de diagnostic comme base pour la prise de décision médicale. Veuillez également noter que votre **prestataires de soins de santé** ne sont pas obligés de vérifier vos données d'activité et n'ont pas à vous donner de commentaires concernant vos données d'activité.

Les données d'activité sont partagées avec vos **prestataires de soins de santé** affiliés chaque fois que l'**application myoncare** est accédée. Vous pouvez révoquer votre consentement au partage des données d'activité à tout moment dans les paramètres de l' **application myoncare**. Veuillez noter que vos données d'activité ne seront plus partagées à partir de ce moment. Les données d'activité qui ont déjà été partagées ne seront pas supprimées du **portail myoncare** de vos **Prestataires de soins de santé SERV** affiliés.

Le traitement des données d'activité relève de votre propre responsabilité.

Types de données : Le type et la quantité de données transférées dépendent de votre décision et des données disponibles dans votre application Santé connectée. 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 : Vos données d'activité seront mises à la disposition de vos **prestataires de soins de santé** avec qui vous êtes connecté dans le but de fournir des informations supplémentaires et contextuelles concernant votre activité.

Justification du traitement : Le traitement des données d'activité relève de votre propre responsabilité.

TRAITEMENT DES DONNÉES DE SÉCURITÉ DES PRODUITS
Applicable aux utilisateurs de l'application dont le fournisseur de services utilise la variante de dispositif médical des outils myoncare

L' **application myoncare** est classée et commercialisée en tant que dispositif médical conformément à la réglementation européenne sur les dispositifs médicaux. En tant que fabricant de l'application, nous devons respecter certaines obligations légales (par exemple, surveiller le fonctionnement de l'application, évaluer les rapports d'incident qui pourraient être liés à l'utilisation de l'application, suivre les utilisateurs, etc.). De plus, l'**application myoncare**permet **à** vous et votre **fournisseur de santé** de communiquer et collecter des données personnelles concernant certains dispositifs médicaux ou médicaments utilisés dans votre traitement. 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 déclarations d'effets indésirables).

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

Traitement des données de sécurité du produit : Nous stockerons et évaluerons toutes les données personnelles liées à nos obligations légales en tant que fabricant d'un dispositif médical et transmettrons ces données personnelles (si possible après pseudonymisation) aux autorités compétentes, aux organismes notifiés ou à d'autres contrôleurs de données ayant des obligations de surveillance. De plus, nous stockerons et transférerons des données personnelles liées avec des dispositifs médicaux et/ou des médicaments si nous recevons des notifications de votre **fournisseur de soins de santé**, de votre part en tant que patient ou d'un tiers (par exemple, nos

distributeurs ou importateurs de **myoncare tools** dans votre pays) qui doivent être signalés au fabricant du produit afin que le fabricant puisse se conformer à ses obligations légales en matière de sécurité du produit.

Règles du RGPD

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

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. 9 par. 2 lit. i le RGPD en liaison avec les obligations de surveillance existant après la mise sur le marché en vertu de la loi 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 loi sur les médicaments.

TRAITEMENT DES DONNÉES DE GESTION DE LA SANTÉ AU TRAVAIL

Applicable aux utilisateurs de l'application qui utilisent l'application avec la gestion de la santé au travail de l'entreprise

Lors de l'utilisation de l'**application myoncare** dans la gestion de la santé au travail **de l'entreprise**, certaines données personnelles (de santé) sont transmises sous forme agrégée en tant que données pour la gestion de la santé au travail à l'entreprise et aux **prestataires de services de données** mandaté par l'entreprise (par exemple, des analystes de données ou des sociétés de recherche). Ni l'**entreprise** ni aucun **fournisseur de services de données** ne peuvent attribuer ces données à votre identité. ONCARE recommande de ne pas partager de données personnelles lors de l'utilisation de **services myoncare** dans le cadre de la gestion de la santé au travail.
Cela signifie que ONCARE et tous les **fournisseurs de services de données** ne traiteront les données que pour la gestion de la santé au travail conformément aux instructions de l' **entreprise**. Nous traitons ces données pour la gestion de la santé au travail, y compris vos données de santé, sur la base d'un accord avec l' **entreprise** et/ou d'un **fournisseur de services de données** et conformément à leurs instructions. Aux fins du présent Accord, la Société est le responsable du traitement de vos données de gestion de la santé au travail et de tout **fournisseur de services de données** engagé par votre **entreprise**, le cas échéant, sont les sous-traitants de ces données. Si vous avez des questions ou des préoccupations concernant le traitement de vos données pour la gestion de la santé au travail, vous devez contacter l'entreprise en premier lieu.

Traitement des données: Nous traitons les données de gestion de la santé de votre entreprise afin de pouvoir fournir notre **service myoncare** pour l' **entreprise** et pour vous. Vos données de gestion de la santé au travail, que vous saisissez dans notre **application myoncare**, seront utilisées par l' **entreprise** (soit directement, soit par l'intermédiaire d'un **fournisseur de services de données**) dans le cadre de la gestion de la santé au travail. Nous traitons ces données personnelles dans le cadre d'un accord et conformément aux instructions de votre **fournisseur de soins de santé**. La transmission de ces données de traitement est pseudonymisée et cryptée. Pour exercer vos droits en tant que personne concernée, veuillez vous adresser à votre **fournisseur de services**.

Règles du RGPD
Vos données pour la gestion de la santé au travail seront traitées par l' **entreprise** conformément aux dispositions de la **RGPD** et toutes les autres réglementations applicables en matière de protection des données. La base juridique du traitement des données est, en particulier, votre consentement conformément à l'art. 6 par. 1 lit. a et de l'art. 9 par. 2 lit. a **RGPD** ou une autre norme applicable à l' **entreprise**. Le traitement des données par ONCARE à l' **entreprise** (soit directement, soit par l'intermédiaire d'un **fournisseur de services** commandé par l'**entreprise**) est également fondée sur l'art. 28 **RGPD** (Accord de traitement des données).

L' **entreprise,** en tant que responsable des données, est responsable de l'obtention de votre consentement si la réglementation sur la protection des données l'exige et du traitement des données à des fins de gestion de la santé au travail conformément aux lois applicables en matière de protection des données.

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'email

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 de courriers électroniques. 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 ;
- 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 emails pour les PWA (Progressive Webapp) dans les cas suivants :
(i) Si un plan de soins prend fin dans la journée ;
(ii) si un médicament a été assigné ;
(ii) lorsque la Politique de confidentialité a été mise à jour ;
(iv) lorsqu'un rendez-vous est envoyé aux patients et aux médecins, en particulier pour le type de rendez-vous « appel vidéo » ;
(v)Toutes les informations sur une **CareTask** ou lorsqu'un **fournisseur de soins de santé** a assigné une **CareTask**.

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

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

Matomo
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, à condition que 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 de l'utilisateur ;
- Géolocalisation de l'utilisateur ;
-Navigateur;
- Système d'exploitation utilisateur ;
-Adresse IP;
- Sites visités via web / PWA (pour plus d'informations, voir la section sur les PWA dans la présente politique de confidentialité) ;
- les boutons sur lesquels l'utilisateur clique dans le **Portail myoncare**, dans l' **application myoncare** et dans le **myoncare PWA**;
- le temps d'utilisation du contenu par l'utilisateur.
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 ne traitons et ne conservons les données personnelles qu'aussi longtemps que nécessaire pour atteindre 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 vers et depuis l'application est crypté. Nous utilisons TLS et SSL comme protocoles de cryptage pour le transfert sécurisé 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). Toute transmission de données personnelles est cryptée lors de la transmission.

Nous ne partagerons des informations et des données vous concernant que si l'État ou la loi fédérale des États-Unis l'exigent.; 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. Nous pouvons également traiter et partager vos données de santé afin de :

- le respect des lois fédérales, étatiques ou locales ;
- Fournir un soutien aux activités de santé publique, telles que la maladie ou l'utilisation de matériel médical ;
- Fournir aux autorités des informations pour protéger les victimes de maltraitance ou de négligence ;
- Respect des activités de surveillance de la santé fédérales et étatiques, telles que les enquêtes sur les fraudes ;
- Pour faire respecter les ordonnances des forces de l'ordre ou des tribunaux, les citations à comparaître ou d'autres actions souveraines connexes ;
- Effectuer des recherches sur les protocoles d'examen interne afin d'assurer un équilibre entre la protection de la vie privée et les besoins en matière de recherche ;
- Prévenir une menace grave pour la santé ou la sécurité.

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 d'accorder 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, l' **application myoncare** vous en informera expressément dans le cadre de la procédure de consentement.

Pour le traitement des données pour lequel votre consentement est requis (comme expliqué dans la présent e**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 de l'**application myoncare**.

Règles du RGPD

Traitement de catégories particulières de données à caractère personnel conformément à l'art. 9 par. 1 Le RGPD ne peut avoir lieu que si la loi l'exige 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.

DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Au sein de notre organisation, nous veillons à ce que seules les personnes autorisées à traiter les données personnelles nécessaires à l'exécution de leurs obligations contractuelles et légales. Vos données personnelles et les données de santé que vous saisissez dans notre **application myoncare** seront mises à la disposition de votre **fournisseur de soins de santé** et/ou **entreprise** soit directement, soit par l'intermédiaire d'un **fournisseur de services de données** (selon le type d'utilisation des **outils myoncare**).
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 des données personnelles. Ces fournisseurs de services sont Google (Google Firebase), Fournisseurs de stockage dans le cloud et fournisseurs de services d'assistance.
Google Firebase est une « base de données NoSQL » qui permet la synchronisation entre vos **Portail du fournisseur de santé myoncare**et l' **application myoncare**. 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 cette fin, une pseudo-clé de l' **application myoncare** est stockée dans Google Firebase ainsi que le Care Plan 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. Ceci est réalisé en cryptant les données lors du transfert entre vous et vos **prestataires de soins de santé** ou **votre entreprise** (soit directement, soit vers n'importe quel **fournisseur de services de données**) et en utilisant des pseudo-clés au lieu d'identificateurs personnels tels que le nom ou l'adresse e-mail pour suivre ces transferts. La réidentification a lieu dès que les données personnelles ont atteint le compte de votre **prestataires de soins de santé** ou **de votre entreprise** sur le **portail myoncare** ou votre compte dans l' **application myoncare**, après avoir été vérifié par des tokens spécifiques.

Nos fournisseurs de stockage dans le cloud proposent une gamme de services de stockage dans le cloud dans lequel le gestionnaire Firebase, qui gère les URL Firebase pour le **portail myoncare**, est stocké. De plus, ces prestataires de services fournissent le domaine de serveur isolé du **portail myoncare**, dans lequel vos données personnelles sont stockées. Il héberge également les services de gestion de vidéos et de fichiers de myoncare, qui permettent des vidéoconférences cryptées entre vous et votre **Fournisseur de soins de santé** ainsi que l'échange de fichiers. Accès à vos données personnelles par vous et vos **fournisseurs de soins de santé** est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées pendant le transfert et au repos et pseudonymisées pour ONCARE et ses prestataires de services. 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 spécialement agréé par ONCARE, 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

TRANSFERTS 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 ne seront transférées vers des pays tiers 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 de la fonction **L'application MyonCare** et le **Portail MyonCare** se déroule via Google Firebase. Le serveur Google Firebase est hébergé dans l'Union européenne. Toutefois, comme décrit dans les Conditions d'utilisation de Google Firebase, des transferts de données à court terme vers des pays dans lesquels Google ou ses fournisseurs de services sont situés sont possibles. 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 illégal à vos données est empêché par un cryptage de bout en bout et des 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, adresse IP, informations du navigateur, 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 vers les services Google Cloud (dans le cas de GoogleFit) ou vers AppleHealth ou Withings sont utilisées au sein de l'appareil mobile de l'**utilisateur de l'application**. **Outils**

MyonCare utiliser ces interfaces, qui sont fournies par Google, Apple et Withings, pour demander des données d'activité aux applications de santé connectées. L'enquête envoyée par **outils myoncare** 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 (par exemple le Code de commerce, la loi fiscale, etc.). De plus, votre **fournisseur de soins de santé** doit également assurer la conservation de votre dossier médical (entre 1 et 30 ans, selon le type de documents).
De plus, et seulement si votre **fournisseur de soins de santé** utilise la variante dispositif médical des **outils myoncare**, certaines périodes de conservation résultant de la loi sur les dispositifs médicaux s'appliquent en raison de la classification de l'**application myoncare** en tant que dispositif médical. Veuillez noter qu'ONCARE est également soumis à des obligations de conservation convenues contractuellement avec votre **fournisseur de soins de santé** sur la base des dispositions légales. 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 **L'application MyonCare** et les différentes fonctions qu'il offre.

Nous avons résumé les détails pour vous sous le point ci-dessus. 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.

DROITS D'ACCÈS

Pour que l' **application myoncare** fonctionner sur votre appareil, l'application doit disposer de diverses autorisations pour accéder à certaines fonctions de l'appareil. Pour tous les appareils, quel que soit le système d'exploitation utilisé, il est nécessaire d'accorder à l'application certaines autorisations, que nous appelons « droits d'accès de base ». Le cas échéant, nous les listerons dans l'ordre du système d'exploitation (Android ou iOS) selon les « conditions de base ». Selon le système d'exploitation de l'appareil que vous utilisez, il peut avoir des fonctionnalités supplémentaires qui nécessitent des autorisations supplémentaires pour que l'application fonctionne.

Les droits d'accès de base (Android et iOS) sont les suivants :

Obtenir des connexions Wi-Fi
Nécessaire pour assurer la fonctionnalité du téléchargement de documents en conjonction avec les connexions Wi-Fi.

Obtenir une connexion réseau
Requis pour assurer la fonctionnalité du téléchargement de documents en conjonction avec des connexions réseau qui ne sont pas des connexions Wi-Fi.

Désactiver le verrouillage de l'écran (empêcher le mode veille)
Nécessaire pour que les vidéos qui appartiennent aux documents fournis puissent être lues directement dans l'application sans être interrompues par un verrouillage de l'écran.

Accès à tous les réseaux
L'accès à tous les réseaux est requis pour télécharger les documents.

Désactiver le mode veille
Cela est nécessaire pour que les vidéos qui appartiennent aux documents fournis puissent être lues directement dans l'application sans que la lecture ne soit interrompue par l'apparition d'une mise en veille prolongée.

Données mobiles / Accès aux données mobiles
Si l'utilisateur souhaite télécharger des documents exclusivement via Wi-Fi, il peut effectuer le réglage approprié dans le menu de l'application et désactiver l'utilisation des données mobiles. L'accès aux données mobiles est nécessaire pour garantir la fonctionnalité de désactivation des téléchargements de documents sur les données mobiles.

Accès à l'appareil photo
L'accès à la caméra est nécessaire pour scanner les QR codes ainsi que pour les consultations vidéo.

Accès au microphone
L'accès au microphone est requis pour les consultations vidéo.

Accès aux fichiers et aux photos
Ceci est nécessaire pour l'échange de fichiers entre vous et les utilisateurs de votre portail connecté.

Accès aux navigateurs web
Requis pour visualiser les fichiers reçus par les utilisateurs du portail connectés.

Nous utilisons des notifications push, qui sont des messages envoyés à votre appareil mobile en tant que service de l' **application myoncare** via des services tels que Apple Push Notification Service ou Google Cloud Messaging Service. Ces services sont des fonctionnalités standard des appareils mobiles. La politique de confidentialité du fournisseur de services régit l'accès, l'utilisation et la divulgation des renseignements personnels à la suite de votre utilisation de ces services.

DÉCISIONS AUTOMATISÉES DANS DES CAS INDIVIDUELS CONFORMÉMENT AU RGPD

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

VOS DROITS EN VERTU DE L'HIPAA

Sous **HIPAA**, vous disposez des droits suivants :

- Consulter et copier certaines parties de vos renseignements sur la santé. Vous pouvez demander à ce que vos données de santé soient mises à votre disposition sous forme électronique. Une copie ou un résumé de vos renseignements sur la santé vous sera fourni, généralement dans les 30 jours suivant votre demande. Des frais de traitement raisonnables peuvent être facturés.

- Vous pouvez demander que le contenu de vos renseignements sur la santé soit modifié si vous estimez que les renseignements sur la santé sont inexacts ou incomplets. Vous pouvez demander la correction de renseignements sur la santé si vous croyez qu'ils sont inexacts ou incomplets.

- Établissez des divulgations obligatoires de vos renseignements sur la santé au cours des six dernières années, avec des restrictions sur le traitement, le remboursement et le traitement. Des frais de traitement raisonnables peuvent être facturés.

- Vous pouvez demander à ce que certaines informations de santé, y compris les traitements, les paiements de redevances ou d'autres sujets médicaux, ne soient pas utilisées ou partagées.

- Vous pouvez demander une copie papier de la politique de confidentialité à tout moment, même si vous avez accepté de recevoir l'avis uniquement par voie électronique.

- Déposez une plainte auprès de l'autorité compétente si vous estimez que vos droits en matière de protection des données ont été violés. Vous pouvez déposer une plainte auprès du Ministère de la Santé et des Services sociaux des États-Unis., par courrier postal à l'adresse suivante : 200 Independence Avenue, S.W., Washington, D.C. 20201, par téléphone au 1-800-368-1019 (sans frais) ou au 1-800-537-7697 (ATP), ou en visitant le https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf .

De nombreux états des États-Unis ont promulgué leurs propres lois pour protéger les droits des patients, qui s'appliquent aux patients des médecins et/ou des hôpitaux et autres établissements de santé. Certains de ces états des États-Unis exigent des médecins qu'ils

fournissent une copie de ces droits des patients à leurs patients.

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 à l'information (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 l'**application myoncare**, y compris votre UID (numéro d'identification unique) de votre smartphone/appareil mobile.

Droit de rectification (art. 16 du RGPD) : Vous pouvez nous demander de mettre à jour ou de corriger des données personnelles inexactes 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 contacter en premier lieu votre **fournisseur de soins de santé** ou **votre entreprise** ou contactez-nous à l'adresse suivante : 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.

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. Secrétaire à la Santé et aux 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

Pour déposer une plainte auprès du Ministère de la Santé et des Services sociaux des États-Unis, écrivez au 200 Independence Ave., S.W., Washington, D.C. 20201 ou composez le 1-800-368-1019 (sans frais) ou le 1-800-537-7697 (DTT) ou déposez une plainte en ligne à

l'adresse suivante : https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

DÉLÉGUÉ À LA PROTECTION DES DONNÉES SELON LE 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 .

RESTRICTION D'ÂGE DE L'APPLICATION

Un âge minimum de 18 ans est requis pour utiliser l' **application myoncare**. Si vous avez moins de 18 ans, votre parent ou tuteur doit fournir le consentement à la confidentialité requis pour utiliser l'application.

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**.
Les 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 révisée lors de la connexion ou en informant 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

Dernière mise à jour le 20 Février 2025

* * * *