Bienvenue sur myoncare, le portail de santé numérique et l'application mobile («**App**») pour une prise en charge efficace et adaptée aux besoins des patients et un soutien à la gestion de la santé au travail.

Cette politique de confidentialité est divisée en deux parties :

- La première partie contient les règles de protection des données pour l'utilisation de la plateforme myoncare en Europe conformément au **Règlement général sur la protection des données (RGPD) de l'UE.**

- La deuxième partie contient **Informations complémentaires** conformément aux exigences de la **la loi sur la protection des données des États-Unis d'Amérique (HIPAA),** en particulier pour les utilisateurs résidants aux États-Unis ou en cas de traitement de données de santé par des prestataires de soins de santé américains.

Pour nous, chez Oncare GmbH (ci-après dénommée «**ONCARE"** ou «**nous**", **« Nous**", "**notre**»), la protection de votre vie privée et de toutes les données personnelles vous concernant lors de l'utilisation de l' **App** est d'une grande importance et 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. Dans cette politique de confidentialité, vous apprendrez 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 aurez 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.

1. DÉFINITIONS

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

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

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

"**Fournisseur de services de données**» désigne tout agent engagé et chargé par l'entreprise 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.

"**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 tâches de soins, éventuellement séquencées dans le temps, qui permettent de déterminer les étapes du diagnostic et des thérapies.

« Care tasks » 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 l'application myoncare et le portail myoncare.

"**myoncare PWA** » désigne l'application myoncare Progressive Web App pour les patients qui souhaitent utiliser les services proposés par ONCARE par l'intermédiaire de la PWA et non par l'intermédiaire de 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 utilisant 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.

2. TRAITEMENT DES DONNÉES (OPÉRATIONNELLES)

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**. 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** .

3. 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 qui divulguent des informations sur 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.

4. 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 capacités natives des appareils mobiles sans avoir besoin d'un magasin d'applications. L'objectif des PWA est de combiner la différence entre les applications et le Web traditionnel en apportant les avantages des applications mobiles natives au navigateur. La PWA est basée sur la technologie de « React ». « React » est un logiciel open source pour les applications PWA.

Pour utiliser le **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.

Les informations suivantes sur l' **application myoncare** s'applique également à la **myoncare PWA**, sauf indication contraire dans le présent article.

5. 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 care plan). Les renseignements relatifs à votre traitement comprennent, sans s'y limiter : des renseignements sur les médicaments pris, les réponses aux questionnaires, y compris des renseignements liés à la maladie ou à l'affection, les diagnostics et les thérapies fournis par votre **fournisseur de soins de santé** , les tâches planifiées et terminées.

Données du magasin commercial : Données du magasin commercial : Données à caractère personnel traitées dans le cadre de l'utilisation du myoncare Store – en particulier dans le cadre de la paternité, de la configuration ou de l'achat de plans de traitement numériques (« Pathways »). Le magasin est exploité par myon.clinic GmbH, une filiale d'Oncare GmbH. L'utilisation de la Boutique nécessite le traitement de votre nom, de vos coordonnées professionnelles et, le cas échéant, de vos données de paiement (uniquement pour les contenus payants). Oncare GmbH traite ces données exclusivement pour la mise à disposition technique des fonctions de la plateforme et non à ses propres fins commerciales.

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 **fournisseurs de service** 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.

Utilisation des données anonymisées à des fins commerciales : En outre, ONCARE peut utiliser certaines données de santé et d'utilisation, une fois entièrement anonymisées, à des fins commerciales, telles que l'amélioration de la plateforme, l'analyse des processus de soins ou le développement de nouveaux services de santé numériques. L'anonymisation est effectuée de manière à ce que les individus ne puissent plus être identifiés. Ces données anonymisées ne sont donc plus soumises au RGPD.

Données provenant de fabricants de dispositifs, de distributeurs de dispositifs médicaux ou de laboratoires :
En outre, les données à caractère personnel peuvent être traitées par des fabricants de dispositifs médicaux connectés, des distributeurs de dispositifs médicaux ou des prestataires de services de laboratoire dans le cadre de processus de soins intégrés, à condition qu'elles soient commandées ou utilisées par le prestataire de services via le portail myoncare.

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 entreprises de dispositifs médicaux ou pharmaceutiques à des fins de sécurité juridique ou de vigilance.

Données de remboursement : Données personnelles nécessaires au processus de remboursement entre votre fournisseur 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 encore des données sur les soins ou la santé en général.

6. 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 services** 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 de blockchain.

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

En général, la **blockchain** se compose de données numériques dans une chaîne de paquets appelés « blocs » qui stockent les transactions correspondantes. La façon dont ces blocs sont reliés les uns aux autres est chronologique. Le premier bloc créé est appelé bloc de genèse, et chaque bloc ajouté par la suite a un hachage cryptographique lié au bloc précédent, de sorte que les transactions et les modifications d'informations peuvent être retracées 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 pour 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**. Lorsque tous les nœuds (nœuds du réseau) tentent de synchroniser leurs copies, il détecte qu'une copie a été modifiée et le réseau considère ce nœud comme défectueux.

Notre **blockchain** est une **blockchain** privée. Une **blockchain** privée est décentralisée. Il s'agit d'un système dit de registre distribué qui agit comme une base de données fermée. Contrairement au public **Blockchains**, qui sont « non autorisés », privés **Blockchains** sont « autorisés » parce qu'une autorisation est requise pour devenir un utilisateur. Contrairement aux **Blockchains** publiques, qui sont accessibles à tous, accès aux **Blockchains** dépend de l'éligibilité à 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, notamment, en respectant la réglementation du Règlement général sur la protection des données (RGPD). Les enregistrements privés de la blockchain peuvent être modifiés, modifiés ou supprimés. Dans ce contexte, la suppression signifie que la valeur de référence à l'UUID (Universally Unique Identifier) dans le service **du fournisseur de** la base de données est supprimée. En outre, 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
- UUID du patient
- 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 et privées ; Le processus d'enregistrement génère des certificats qui sont stockés dans une base de données distincte du **fournisseur** et sur le téléphone portable du patient. Une copie de sauvegarde de la clé du patient est chiffrée et stockée dans le **fournisseur** de base de donnée, qui n'est accessible qu'au patient.

Lors de la vérification du consentement à la protection des données, dans le cas où le **fournisseur** souhaite communiquer avec le Patient, le système vérifie si le Patient a donné son consentement à la Politique de confidentialité du Fournisseur. 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 donné son consentement, 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 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 **prestataire de services obtient** une actualité suffisante en ce qui concerne le profil du patient.

Portail myoncare:

Si le **fournisseur de services** choisit 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 compte du **fournisseur de services** est effectué sur la base de l'art. 28 du RGPD (Accord sur le traitement des données).

7. TRAITEMENT DES DONNÉES OPÉRATIONNELLES

Applicable à tous les utilisateurs de l'application

Vous pouvez nous fournir certaines données personnelles lorsque vous nous contactez pour comprendre les fonctions et l'utilisation de l' **application myoncare** , en cas de demande de service de votre part ou dans le cas d'une offre d'assistance initiée par nos soins (par téléphone).

Employés de service
Pour le compte du responsable du traitement des données (par ex. Nous vous proposons une assistance pour remplir des questionnaires par téléphone (appels sortants) afin d'optimiser votre prise en charge numérique des patients. Si vous ne souhaitez pas profiter de cette offre, vous êtes libre de ne pas l'accepter et de vous opposer à l'assistance téléphonique.

En cas de demande de service et 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 services** via notre application (par exemple, nom, date de naissance, photo de profil, coordonnées).

- Les données de santé que vous avez fournies à votre **prestataire de soins,** prestataire de **services de données** ou à votre **employeur** via notre **application myoncare** (par exemple, des informations sur les médicaments pris, les réponses à des questionnaires incluant des informations liées à une maladie ou un état de santé, les diagnostics et thérapies des professionnels de santé, les tâches planifiées et réalisées).

Les employés autorisés d'ONCARE qui peuvent accéder à la base de données de votre fournisseur de services**,** fournisseur de services de données **ou** employeur **dans le but de traiter une demande de service ou 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 de 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** (WebApp progressive) 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 au courant de vos tâches et des mises à jour importantes pour soutenir votre santé de la meilleure façon possible.
- 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 une réception fluide de nos messages.
- Si vous ne souhaitez pas recevoir de rappels par e-mail, vous pouvez les désactiver dans les paramètres de l'application myoncare.

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

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

Types de données: 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 ; Jetons 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.

Lorsque l' **application myoncare** est téléchargée, les informations nécessaires sont transmises au fournisseur de l'App Store. Nous n'avons aucune influence 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** et services myoncare.

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 de vous contacter directement si nécessaire ou à l'initiative de vos soins (par exemple en cas de modifications des conditions générales, d'assistance nécessaire, de problèmes techniques, d'assistance pour remplir les questionnaires, etc.).

Justification du traitement: Le traitement des données de l'entreprise est justifié sur la base de l'art. 6 (1) (b) du RGPD pour l'exécution du contrat que vous concluez avec ONCARE dans le but d'utiliser l'**application myoncare** .

8. 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 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 informations de localisation. La base juridique de l'utilisation est l'art. 6 par. 1 lit. f RGPD. Les données seront supprimées lorsque la finalité pour laquelle elles ont été collectées n'existe plus et qu'il n'existe plus d'obligation légale de les conserver. Pour plus d'informations sur leurs politiques de confidentialité, veuillez visiter https://ipapi.com/privacy/

9. TRAITEMENT DES DONNÉES (OPÉRATIONNELLES)

Applicable aux utilisateurs de l'application qui utilisent l'application avec leur fournisseur de services.

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 services peut télécharger** documents et dossiers à l' **application myoncare** et le **portail myoncare** et les partager les uns avec les autres. Votre **fournisseur** peut télécharger une **politique de confidentialité** pour votre information et établir d'autres exigences en matière de consentement pour vous en tant que patient pour lesquelles votre consentement est requis. Les fichiers sont stockés dans une base de données cloud en Allemagne. Votre **fournisseur de services** peut permettre le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de son institution ou d'autres **fournisseurs** à l'extérieur de son établissement (médecins consultants) à des fins médicales. Les autres utilisateurs du portail n'auront pas accès à ces fichiers sans ce partage. De plus, votre **fournisseur de services** peut nous demander de vous aider par téléphone à remplir des questionnaires (appels sortants). Cela se fait uniquement selon les instructions de votre fournisseur de services et est effectué exclusivement par des employés autorisés d'ONCARE.

Nous utiliserons et traiterons vos données conformément aux **conditions énoncées dans la présente politique de confidentialité**, à condition que vous nous donniez votre consentement le cas échéant.

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**. Pour ces finalités de traitement, le **fournisseur de services** est responsable du traitement de vos données personnelles et de vos données de santé en tant que responsable du traitement des données au sens des lois applicables en matière de protection 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 services**. Si vous avez des questions ou des préoccupations concernant le traitement de vos données personnelles ou de vos données de santé, vous devez d'abord contacter votre prestataire de soins de santé.

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 par des professionnels de la santé, des tâches planifiées et réalisées.

Finalités du traitement des données : Nous traitons vos données de traitement afin de fournir notre **Service myoncare** à votre **fournisseur de services** et à vous. Vos données de santé, que vous saisissez dans notre **application myoncare** , seront utilisées par votre **fournisseur de services** 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 services**. La transmission de ces données de traitement est pseudonymisée et cryptée. Pour exercer vos droits en tant que personne concernée, veuillez vous adresser à vos **fournisseurs**.

Justification du traitement des données de traitement : Vos données personnelles (de traitement) seront traitées par votre **fournisseur de services** 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 (2) (h) du RGPD pour les données de santé en tant que données particulièrement sensibles ainsi que votre consentement conformément à l'art. 6 (1) (a) et 9 (2) (a) du RGPD. Le traitement des données par ONCARE pour son **fournisseur de soins de santé** est également effectuée sur la base de l'art. 28 du RGPD (Accord sur le traitement des données).
Votre **fournisseur de services** est responsable de l'obtention de votre consentement en tant que responsable du traitement des données. 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). Le refus ou la révocation du consentement au traitement des données de traitement entraîne

donc une restriction sévère de la fonctionnalité des services de l'application et de vos **fournisseurs de service** ne peut plus vous soutenir via l' **application myoncare**.

10. 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 («**Application Santé**"). Afin de permettre le traitement des données d'activité, nous obtenons au préalable votre consentement au traitement. Si la connexion est établie après votre consentement, les **données d'activité collectées** par l'**application Santé** seront mis à la disposition de vos prestataires pour vous fournir des informations contextuelles supplémentaires sur votre activité. Veuillez noter que les données d'activité ne sont pas validées par **outils myoncare** et ne doivent pas être utilisées par votre **fournisseur de soins de santé** à des fins de diagnostic comme base de décision médicale. Veuillez également noter que vos **fournisseurs** ne sont pas tenus de vérifier vos données d'activité et n'ont pas à vous fournir de commentaires sur vos données d'activité.
Les données d'activité sont partagées **avec votre affilié** chaque fois que l' **application myoncare** est accessible . Vous pouvez révoquer votre consentement à la divulgation 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 **fournisseurs de services affiliés**.

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

Types de données : Le type et la quantité de données transférées dépendent de votre décision et de la disponibilité de ces données dans l'**application 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 fournies à vos **fournisseurs** affiliés pour fournir des informations contextuelles supplémentaires sur votre Activité.

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

11. TRAITEMENT DES DONNÉES DE SÉCURITÉ DU PRODUIT

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

L'**application myoncare** est classé et commercialisé 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** vous permet, à vous et à votre **fournisseur de soins de santé** pour communiquer et recueillir des informations personnelles sur des dispositifs médicaux ou des médicaments spécifiques 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 rapports sur les effets secondaires).

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

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

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 (dans la mesure du possible après pseudonymisation) aux autorités compétentes, aux organismes notifiés ou à d'autres responsables du traitement des données ayant des fonctions de surveillance. En outre, nous stockons et transférons des données personnelles relatives aux dispositifs médicaux et/ou aux médicaments lorsque nous recevons des communications de votre **fournisseur de soins de santé**, de votre part en tant que patient ou de tiers (par exemple, nos distributeurs ou importateurs des **outils myoncare** dans votre pays) qui doivent être signalés au fabricant du produit afin qu'il soit conforme 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 produits pharmaceutiques est l'art. 6 1) c), art. 9 (2) (i) du RGPD en liaison avec les obligations de surveillance post-commercialisation 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.

Complément à l'exclusion de responsabilité pour les effets secondaires :
Oncare GmbH ne procède à aucune évaluation médicale des contenus transmis et n'est pas tenue de transmettre aux autorités des informations pertinentes pour le droit pharmaceutique telles que les effets secondaires, les erreurs d'application ou les défauts du produit. Cette responsabilité incombe exclusivement aux prestataires de services traitants ou, le cas échéant, aux fabricants respectifs des produits utilisés.

12. TRAITEMENT DES DONNÉES DE SANTÉ ET DE TRAITEMENT

Applicable aux utilisateurs de l'application qui utilisent l'application avec leur fournisseur de services à des fins de remboursement.
L'**application myoncare** soutient votre **fournisseur de soins de santé** en engageant des procédures standard de remboursement des prestations de santé qui vous sont fournies 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 votre **fournisseur de services** dans le but de transmettre ces données à votre entité payeuse (soit l'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 services** pour obtenir le 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 services**. Votre prestataire de services est le responsable du traitement 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 services**.

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** transmet les données de traitement nécessaires au remboursement au payeur (soit son institution d'assurance maladie légale et/ou votre caisse d'assurance maladie), et le payeur traite les données de remboursement afin de rembourser votre **fournisseur** .

Justification du traitement des données de remboursement : Les données de remboursement sont traitées sur la base des §§ 295, 301 SGB V, art. 9 par. 2 lit. b RGPD. Traitement des données par ONCARE pour votre **fournisseur de services** est également effectué sur la base de l'art. 28 du RGPD (accord de traitement des commandes).

13. TRAITEMENT PAR LES FABRICANTS DE DISPOSITIFS, LES DISTRIBUTEURS DE DISPOSITIFS MÉDICAUX ET LES PRESTATAIRES DE SERVICES DE LABORATOIRE

Si vous utilisez des fonctions médicales supplémentaires telles que le diagnostic intégré, la collecte de signes vitaux ou les services de laboratoire via la plateforme, les données de santé personnelles peuvent être collectées et traitées par des fournisseurs tiers externes (par exemple, des fabricants de dispositifs médicaux, des distributeurs de ceux-ci ou des prestataires de services de laboratoire). Ceci est fait pour soutenir les soins médicaux et toujours sur la base d'un consentement explicite ou d'une relation de traitement.
Le traitement est effectué soit dans le cadre du traitement de la commande, soit, selon le prestataire, sous sa propre responsabilité en vertu de la loi sur la protection des données. Oncare GmbH ne fournit que la connexion technique à cet effet, sans vérification ni évaluation médicale des contenus. De plus amples informations sur le traitement des données respectif peuvent être obtenues directement auprès du prestataire de services traitants ou via les informations sur la protection des données des fournisseurs tiers intégrés.

14. GESTION DES DONNÉES ET DES PARCOURS DES MAGASINS COMMERCIAUX

Le portail myoncare offre aux prestataires de services enregistrés (par exemple des médecins) la possibilité de proposer et de configurer des parcours de soins numériques via une fonctionnalité de boutique en ligne (par exemple en coopération avec myon.clinic) et d'assigner des patients individuellement.
Dans le cadre de l'utilisation de cette fonctionnalité, des données à caractère personnel, en particulier des données de santé, sont traitées, telles que des informations sur l'indication, la durée recommandée du traitement ou l'attribution d'un pathway. Ce traitement des données sert à l'individualisation et à l'attribution de contenus médicaux et est effectué sur la base de l'art. 6 (1) (b) et l'art. 9 (2) (h) du RGPD.

Oncare fournit l'infrastructure technique et traite les données concernées en tant que responsable du traitement au sens de l'art. 4 n° 7 du RGPD, dans la mesure où le traitement est nécessaire à la fourniture des fonctions de la plateforme. Toutefois, le choix du contenu et la conception médicale des pathways relèvent de la seule responsabilité du prestataire de services concerné.
Dans la mesure où la facturation ou la transmission de données est effectuée à des tiers (par exemple, des bureaux de facturation ou des partenaires de plateforme tels que myon.clinic), ce traitement n'a lieu que sur la base d'accords ou de dispositions légales correspondants.

15. TRAITEMENT DES DONNÉES DE GESTION DE LA SANTÉ AU TRAVAIL

Applicable aux utilisateurs de l'application qui utilisent l'application avec le système de 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 **fournisseurs de données** mandatés **par l'entreprise** (par exemple, des analystes de données ou des sociétés de recherche). Ni l'**entreprise** ni aucun **fournisseur de services de données** peut associer ces données à votre identité. ONCARE recommande **que vous ne partagez aucune donnée personnelle** lors de l'utilisation des services de myoncare dans le cadre de la gestion de la santé au travail.

Cela signifie que ONCARE et tous les **fournisseurs de données** ne traitent les données que pour la gestion de la santé au travail en accord avec les 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 données** et conformément à leurs instructions. Aux fins du présent Accord, l' **entreprise** ou le **fournisseur de données** est le responsable du traitement de vos données à des fins de gestion de la santé au travail, et ONCARE et tous **fournisseurs de données** engagés par l'**entreprise** 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 d'abord contacter l'entreprise **.**

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**. 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 données**) dans le cadre de la 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 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, en particulier, votre consentement conformément à l'art. 6 (1) (a) et l'art. 9 (2) (a) du RGPD ou d'une autre base juridique applicable à l' **entreprise**. Le traitement des données par ONCARE pour le compte de l' **entreprise** (soit directement, soit par

l'intermédiaire d'un prestataire de services mandaté par votre entreprise) est également fondée 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 lorsque 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.

16. QUELLE EST LA TECHNOLOGIE UTILISÉE PAR L'APPLICATION MYONCARE ?

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 de messagerie peuvent être utilisés pour organiser l'envoi d'e-mails. Sendgrid est utilisé pour envoyer des e-mails de confirmation, des confirmations de transaction et des e-mails contenant des informations importantes sur les demandes. Les données que vous saisissez dans le but de recevoir des e-mails seront 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 à l'application web pour la première fois ;
- 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 ;
- Préparation et envoi d'un rapport ;
- Remplacer les notifications push par des e-mails pour **PWA** (Progressive Web App) dans les cas suivants :
  - → si un care plan se termine dans une heure ;
  - → si un médicament a été assigné ;
  - → si la politique de confidentialité a été mise à jour ;
  - → lors de l'envoi d'un rendez-vous aux patients et aux médecins, notamment pour le type de rendez-vous « appel vidéo » ;
  - → Toute information relative à une **CareTask** ou si un **fournisseur** 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 qui échappent au contrôle d'ONCARE. Matomo est initialement désactivé lorsque vous utilisez nos services. Ce n'est que si vous y consentez que votre comportement d'utilisateur sera enregistré de manière anonyme. Si cette option est désactivée, un « cookie persistant » sera stocké, si les paramètres de votre navigateur le permettent. Ce cookie signale à Matomo que vous ne souhaitez pas que votre navigateur soit enregistré.
Les informations d'utilisation collectées par le cookie sont transmises à nos serveurs et y sont stockées afin que nous puissions analyser le comportement des utilisateurs.
Les informations générées par le cookie concernant votre utilisation sont les suivantes :

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

Les informations générées par le cookie ne seront pas partagées avec des tiers.

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

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

Nous traitons et conservons les données personnelles uniquement aussi longtemps qu'elles sont nécessaires à la réalisation de l'objectif visé.

17. TRANSFERT SÉCURISÉ DES DONNÉES PERSONNELLES

Nous utilisons des mesures de sécurité techniques et organisationnelles appropriées pour protéger de manière optimale vos données personnelles stockées chez nous 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 une transmission sécurisée des données. L'échange de données est également crypté et s'effectue à l'aide de pseudo-clés.

18. 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 en transit.

19. 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 que vous ne donniez 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 (1) du RGPD ne peut avoir lieu que si la loi l'exige et qu'il n'y a aucune raison de croire 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 (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.
Une révocation de votre consentement n'est effective que pour l'avenir. Le traitement effectué jusqu'au moment de la révocation reste licite (art. 7 par. 3 du RGPD).

20. DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Dans notre organisation, nous veillons à ce que seules ces personnes soient autorisées à traiter les données personnelles nécessaires à l'exécution de leurs obligations contractuelles et légales. Vos données personnelles et de santé que vous saisissez dans notre **application myoncare** seront mises à la disposition de votre **fournisseur de soins de santé** et/ou votre **entreprise**, soit directement, soit par l'intermédiaire d'un **fournisseur 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 de données personnelles. Ces fournisseurs de services sont Google (Google Firebase), les fournisseurs de stockage dans le cloud et les fournisseurs de services d'assistance.

Google Firebase est une « base de données NoSQL » qui permet la synchronisation entre le **portail myoncare de votre prestataire de services** 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 **medication 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 en transit entre vous et votre **fournisseur de services** ou **entreprise** (soit directement, soit à un **Fournisseur de données**) et l'utilisation de pseudo-clés au lieu d'identificateurs personnels tels que le nom ou l'adresse e-mail pour suivre ces transferts. La ré-identification a lieu dès que les données personnelles ont atteint le compte de votre **fournisseur de services** ou entreprise dans le **portail myoncare** ou votre compte dans l' **application myoncare**, après qu'il ait été vérifié par des jetons spéciaux.

Nos fournisseurs de stockage en nuage proposent le stockage en nuage, qui stocke le gestionnaire Firebase qui gère les URL Firebase pour le **portail myoncare**. De plus, ces fournisseurs de services fournissent le domaine de serveur isolé du **portail myoncare**, où 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 services**, ainsi que le partage de fichiers. Accès à vos données personnelles par vous et votre **fournisseur de services** est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées en transit et au repos et pseudonymisées pour ONCARE et ses prestataires. Les prestataires 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 de traiter les demandes de service ont été formés en conséquence. À la réception de votre demande de service, un numéro de billet vous 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 lorsque vous nous avez contactés seront transmises à l'un des employés autorisés du service externe. Il vous contactera 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, 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 vous montrons du contenu d'Instagram (fournisseur : Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlande) (par exemple, des images, des vidéos ou des publications). Lorsque vous cliquez sur une publication Instagram liée, vous serez redirigé vers Instagram. Instagram peut définir des cookies et traiter les données des utilisateurs.

Lorsque vous visitez une page avec des publications Instagram liées, votre navigateur peut se connecter automatiquement aux serveurs d'Instagram. Cela donne à Instagram 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 attribuer la visite à votre compte utilisateur.

Politique de confidentialité: https://privacycenter.instagram.com/policy

21. 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. Si les données sont transférées vers un pays tiers où la protection des données à caractère personnel n'a pas été jugée adéquate, nous veillerons à ce que des mesures appropriées soient prises conformément au droit national et européen et, le cas échéant, à ce que des clauses contractuelles types appropriées aient été convenues entre les parties au traitement.
Les données personnelles collectées par cette **application myoncare** ne sont pas stockées dans les magasins d'applications. Un transfert de données personnelles vers des pays tiers (en dehors de l'Union européenne ou de l'Espace économique européen) n'a lieu 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 peuvent être effectués vers des pays où Google ou ses fournisseurs de services sont situés. Pour certains services Google Firebase, les données ne sont transférées aux États-Unis que 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 et aux États-Unis pour les clients américains. 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 du contenu d'Instagram fourni par Meta Platforms Ireland Ltd. Si vous cliquez sur une publication Instagram liée, des données personnelles (par exemple, l'adresse IP, les informations du navigateur, les interactions) peuvent être 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. Néanmoins, 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, mais leur efficacité n'est pas toujours 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. En outre, des mesures de protection techniques supplémentaires ont été mises en œuvre, telles que le chiffrement de bout en bout et la restriction d'accès stricte par le biais de jetons basés sur les rôles. Cela permet de sécuriser davantage le transfert de données au sens de l'arrêt « Schrems II » de la CJUE.

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 sur l'appareil mobile de l'utilisateur de l'application. **Outils myoncare** utiliser ces interfaces, fournies par Google, Apple et Withings, pour demander des données d'activité à partir d'applications de santé connectées. La demande envoyée par les **outils myoncare** ne contient aucune donnée personnelle. Les données personnelles sont mises à la disposition des **outils myoncare** via ces interfaces.

22. 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 pas exclusivement, aux obligations de conservation en vertu du droit commercial ou fiscal (par exemple, Code de commerce, 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 services** sur la base des dispositions légales. De plus, et uniquement si votre **prestataire de services utilise** la version dispositif médical des **outils myoncare**, certaines durées de conservation prévues par la loi sur les dispositifs médicaux s'appliquent en raison de la classification de l'**application myoncare** en tant que dispositif médical. Sauf indication contraire, les données personnelles sont systématiquement supprimées dès que l'objectif a 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 régulier est de trois ans.

23. 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 y afférentes. Il en va de même pour l'utilisation de notre application myoncare et des différentes fonctions qu'elle offre.

Nous avons résumé les détails pour vous sous les points mentionnés ci-dessus. Dans certains cas, les données personnelles doivent également être collectées ou mises à disposition conformément à la loi. Veuillez noter que sans la fourniture de ces données personnelles, il n'est pas possible de traiter votre demande ou d'exécuter l'obligation contractuelle sous-jacente.

24. DROITS D'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. Afin que l'**application myoncare** fonctionne sur votre appareil, il est nécessaire de lui donner diverses autorisations pour accéder à certaines fonctions de l'appareil. Si nécessaire, nous les listerons dans l'ordre du système d'exploitation (Android ou iOS) selon le « Framework ».
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 garantir la fonctionnalité de 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.

Désactivation du 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 la lecture du QR code et 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
Ceci est nécessaire pour afficher les fichiers reçus des utilisateurs du portail connecté.

Nous utilisons des notifications push, qui sont des messages envoyés à votre appareil mobile en tant que service de la **L'application MyonCare** par le biais de services tels que le service de notification push Apple ou le service de messagerie Google Cloud. 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.

25. DÉCISIONS AUTOMATISÉES AU CAS PAR CAS

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

26. 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 conservation et 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 (numéro d'identification unique) de votre smartphone/appareil mobile. 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 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 pour faire valoir des droits 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 notre utilisation de vos données personnelles et de retirer votre consentement à tout moment lorsque nous traitons vos données personnelles sur la base de votre consentement. Nous continuerons à fournir nos services même s'ils ne dépendent pas du retrait du consentement. Une révocation n'a d'effet que pour l'avenir. Le traitement effectué jusqu'au moment de la révocation reste licite.

Pour exercer ces droits, veuillez contacter en premier lieu votre **fournisseur de soins de santé** ou **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 demandons de fournir une preuve suffisante de votre identité pour nous assurer que vos droits sont protégés et que vos données personnelles ne seront partagées qu'avec vous et non avec 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.

27. DÉLÉGUÉ À LA PROTECTION DES DONNÉES
Pour toute question relative à la protection des données, vous pouvez contacter notre délégué à la protection des données à l'adresse suivante privacy@myoncare.com.

28. LIMITE D'ÂGE POUR L'APPLICATION

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

29. 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 se conformer à des exigences légales, pour tenir compte de l'évolution technique et économique ou **pour rendre justice aux** intérêts de l'application **ou** des 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).

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

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

Pour les transactions dans le magasin myoncare – en particulier dans le cadre des plans de traitement (pathways) – la responsabilité économique et liée au contenu incombe à myon.clinic GmbH, une filiale d'Oncare GmbH. Dans ce contexte, Oncare GmbH ne fournit que la plate-forme technique.

Dernière mise à jour en juin 2025.

* * *

Voici les dispositions complémentaires en matière de protection des données pour les utilisateurs aux États-Unis d'Amérique :

La loi HIPAA ne protège les informations de santé personnellement identifiables (PHI) que si elles sont traitées dans le contexte des États-Unis. système de santé par une entité conforme à la loi HIPAA – c'est-à-dire une entité couverte ou un partenaire commercial – indépendamment de la citoyenneté ou du lieu de résidence de la personne concernée.

US Politique de confidentialité supplémentaire pour les utilisateurs aux États-Unis d'Amérique (HIPAA)

Portée:
Cette section complète la politique de confidentialité pour les utilisateurs résidant aux États-Unis d'Amérique (USA) ou pour les cas où Protégé Information sur la santé (RPS) est traité conformément à la loi HIPAA (Health Insurance Portability and Accountability Act).

Elle s'applique dans tous les États des États-Unis dans la mesure où ONCARE ou ses partenaires mandatés traitent des données de santé à titre *Associé d'affaires* au nom de *Entités visées* (par exemple, des médecins ou des cliniques) dans le cadre de processus de traitement.

1. Base juridique aux États-Unis

Le traitement des informations personnelles sur la santé aux États-Unis est régie par la **Loi sur la portabilité et la responsabilité de l'assurance maladie de 1996 (HIPAA)** et les modifications subséquentes, y compris, mais sans s'y limiter :

- HIPAA **Règle de confidentialité** (45 CFR Part 160 et sous-parties A et E de la partie 164)
- HIPAA **Règle de sécurité** (Sous-parties A et C de la partie 164)
- **Règle de notification des violations HIPAA** (Sous-partie D de la partie 164)
- et, en outre, la loi HITECH de 2009

Ces réglementations s'appliquent quel que soit l'État des États-Unis dans lequel se trouve le patient ou l'organisme de traitement.

2. Le rôle d'ONCARE en tant qu'associé commercial

ONCARE GmbH et ses sociétés affiliées aux États-Unis agissent exclusivement en tant que **Partenaires d'affaires** au sens de la loi HIPAA lorsqu'ils **fournissent des services en lien avec le traitement des RPS pour le compte de prestataires de soins de santé (Entités visées**). Un Accord de partenariat commercial (BAA) conformément à l'article 45 CFR §164.504(e) régit les obligations de protection des données envers ces entités. Dans ce cadre, ONCARE s'engage à :

- Mise à disposition de la plateforme myoncare (vidéo, communication, suivi)
- Traitement des données techniques et hébergement
- Mise à disposition de fonctions de soutien algorithmique (p. ex. triage)

ONCARE ne fournit pas de **Services médicaux** et **ne prend pas de décisions médicales** au sens d'un diagnostic, d'une thérapie ou d'une prescription.

3. Type de données traitées (PHI)

Aux fins de la loi HIPAA, les RPS sont définis comme toutes les informations qui :

- se rapportent à l'état de santé ou au traitement d'un patient identifiable, et
- dans le cadre d'une *Entité visée* ou son Associé.

Les RPH traités par ONCARE comprennent notamment :

- Antécédents médicaux (symptômes, facteurs de risque)
- Données de surveillance (signes vitaux, données des objets connectés)
- Interactions avec les utilisateurs au sein de questionnaires structurés ou d'outils de triage
- Historiques de communication avec les prestataires de soins de santé

4. Droits des patients en vertu de la loi HIPAA

Tous les utilisateurs concernés aux États-Unis a le droit de :

- **Information** sur les RPS stockés à son sujet (45 CFR §164.524)

- **Correction** de PHI incorrects ou incomplets (45 CFR §164.526)
- **Limitation** de divulgation ou d'utilisation dans certains cas (45 CFR §164.522)
- **Communication confidentielle** à la demande du patient
- **S' opposer** à certaines divulgations (dans la mesure permise par la loi)
- **Comptabilité** des divulgations (45 CFR §164.528)
- **Plainte** aux États-Unis Ministère de la Santé et des Services sociaux (Office des droits civils)

ONCARE met à disposition sur demande des interfaces techniques permettant la mise en œuvre de ces droits.

Pour faire valoir ces droits, vous pouvez faire une demande informelle via l'application myoncare ou nous contacter par e-mail. La mise en œuvre a généralement lieu dans les 30 jours, conformément à 45 CFR §164.524 et suivants. Si la demande est complexe, le délai peut être prolongé une fois de 30 jours supplémentaires. À cet effet, ONCARE fournit des formats d'exportation numériques et des interfaces d'accès.

5. Mesures de sécurité conformes à la règle de sécurité

ONCARE s'engage à se conformer à toutes les exigences de la règle de sécurité HIPAA, y compris :

Mesures administratives

- Concepts internes de protection des données et d'accès
- Directives écrites sur la réglementation de l'accès
- Analyses de risques et audits réguliers
- Formation des employés axée sur la loi HIPAA

De plus, ONCARE s'engage à effectuer régulièrement une « évaluation des risques de sécurité » structurée conformément au 45 CFR §164.308(a)(1)(ii)(A) afin d'identifier, d'évaluer et de prendre les mesures appropriées à cet égard.

Mesures techniques

- Chiffrement de tous les PHI au repos et en transit
- Contrôle d'accès basé sur les rôles
- Historique de journalisation et d'accès
- Authentification à deux facteurs pour le personnel médical

Mesures physiques

- Emplacements de serveurs sécurisés avec contrôle d'accès
- Concepts de reprise après sinistre
- Restrictions d'accès au matériel et aux terminaux

6. Protection des données dans le triage automatisé

La plateforme myoncare contient une fonction de triage structurée qui évalue les informations sur le patient (par exemple, les symptômes) sur la base de critères définis et crée **une évaluation des risques techniques**.

Cette caractéristique :

- **ne remplace pas un diagnostic médical**,
- **ne décide pas de manière indépendante du traitement ou de l'intervention**,
- **n'informe que les prestataires de services autorisés** (entités visées) d'informations potentiellement pertinentes.

ONCARE n'assume aucune responsabilité médicale pour les décisions prises par les médecins ou les cliniques sur la base de ces informations.

7. Divulgation des RPS et autres utilisations

ONCARE ne partage les RPS qu'avec :

- aux prestataires de soins éligibles dans le cadre des soins,
- aux autorités de contrôle si la loi l'exige,
- pour les incidents de sécurité en vertu de la **Règle de notification des atteintes à la vie privée** (dans les 60 jours suivant la connaissance conformément à 45 CFR §164.404),
- Jamais à des fins publicitaires, de distribution ou d'utilisation par des tiers sans le consentement exprès et documenté du patient.

Toute divulgation ou utilisation des RPS à des fins de recherche, de marketing ou à d'autres fins de tiers n'aura lieu qu'après une autorisation préalable documentée conformément au 45 CFR §164.508. Sans ce consentement exprès, une telle divulgation n'aura pas lieu.

Utilisation de données anonymisées à des fins commerciales
ONCARE peut utiliser des données de santé et d'utilisation qui ont été anonymisées conformément à la règle de confidentialité HIPAA (45 CFR §164.514) à des fins d'analyse interne, d'amélioration de la plateforme, de développement de nouveaux services de santé et à d'autres fins commerciales.

Une fois les données anonymisées, elles ne sont plus considérées comme des informations de santé protégées (PHI) et ne sont pas soumises aux protections de la règle de confidentialité HIPAA.

8. Contact pour l'exercice des droits

Responsable des préoccupations liées à la loi HIPAA :
ONCARE GmbH
Balanstraße 71a80339 MunichAllemagneE-mail : privacy@myoncare.com

Les citoyens américains peuvent également s'adresser au **Ministère de la Santé et des Services sociaux aux États Unis– Bureau des droits civils (OCR)** directement avec les plaintes : https://www.hhs.gov/ocr/

9. Intégration de fournisseurs tiers, données de la boutique en ligne et clause de non-responsabilité

9.1 Implication de prestataires techniques tiers (fabricants de dispositifs, distributeurs de dispositifs médicaux et laboratoires)

Dans le cadre de la plateforme myoncare et de sa filiale myon.clinic, **fournisseurs tiers tels que les fabricants de dispositifs, les distributeurs de dispositifs médicaux ou les laboratoires médicaux** peuvent eut être connectés au système si nécessaire. Ceci est fait exclusivement pour soutenir des soins médicalement responsables et est basé sur les instructions des *Entités visées*.

Les fournisseurs de services tiers connectés traitent les informations de santé personnellement identifiables (PHI) uniquement dans le cadre d'un accord contractuel et conformément aux exigences HIPAA. Vous êtes également soumis aux exigences de protection des données du 45 CFR §164.502(e) en tant que *sous-traitant* d'un partenaire commercial et sont liés par **contrats de sous-traitance (sous-BAA**).

9.2 Collecte de données dans le cadre des offres de la boutique en ligne

Lors de l'achat de programmes de santé numériques, ce que l'on appelle les programmes de santé numériques. **Pathways**, ou des produits affiliés via la boutique en ligne de la filiale **myon.clinic**, les données personnelles, y compris les RPS, peuvent être traitées dans le but de traiter et de maintenir ces programmes. Cela s'applique en particulier :

- Données d'utilisation de la fonctionnalité Pathway,
- données de symptôme ou de diagnostic spécifiées,
- tout code de santé ou information sur le produit échangé.

La collecte est effectuée dans le respect des règles de confidentialité et de sécurité HIPAA et exclusivement dans un but spécifique. La divulgation à des fournisseurs tiers n'aura lieu que sur la base d'un sous-BAA existant ou avec un consentement documenté.

Toute divulgation de PHI (Protected Health Information) en dehors de la chaîne contractuelle (par exemple pour la recherche ou le marketing) nécessite une **« autorisation »** selon 45 CFR §164.508.

9.3 Avis de non-responsabilité pour l'évaluation médicale et les effets secondaires

ONCARE GmbH et ses sociétés affiliées n'assument **aucune évaluation médicale ou obligation de signaler les effets indésirables d'un médicament, les effets secondaires d'un produit ou d'autres risques liés à la santé.**

Responsabilité légale pour :

- le diagnostic et la sélection d'une filière ou d'un produit,
- l'évaluation des risques ou des contre-indications,
- ainsi que la **déclaration obligatoire des effets secondaires** ou des événements de sécurité aux autorités réglementaires ou aux fabricants

incombe exclusivement au médecin traitant ou à l'offrande **Entité visée** ou le fabricant responsable de l'appareil ou du médicament.

La plateforme **ne fournit que l'infrastructure technique** et n'assume aucune responsabilité médicale ou réglementaire quant au contenu, aux résultats ou aux conséquences de toute application par les patients ou les prestataires de services.

Règle de préemption et conformité à la loi de l'État

La loi HIPAA (Health Insurance Portability and Accountability Act) prévoit un **niveau minimal de protection des données en vertu du droit fédéral** qui s'applique dans tous les États-Unis. Dans le même temps, le 45 CFR §160.203 permet ce que l'on appelle **préemption**, c'est-à-dire que des réglementations plus strictes de la part de certains États peuvent l'emporter sur la HIPAA à certains égards si elles :

- assurer une meilleure protection des personnes concernées, ou
- Exigences particulières pour les données de santé ou les données de santé électroniques.
- ONCARE et ses sociétés affiliées s'engagent expressément à se conformer à toutes les lois fédérales pertinentes, y compris, mais sans s'y limiter :

- **Loi californienne sur la protection de la vie privée des consommateurs (CCPA/CPRA)**
- **Loi sur la confidentialité médicale du Texas (TMPA)**
- **Loi SHIELD de New York**
- **Réglementations sur la sécurité des données du Massachusetts**
- ainsi que des lois comparables sur la protection des données au niveau national

Dans la mesure où ONCARE agit pour le compte des entités couvertes, le traitement est effectué conformément à la fois à la loi HIPAA et aux normes de protection des données des États applicables, à condition que celles-ci soient plus strictes que les exigences de la loi HIPAA. En cas d'écart, le règlement qui **offre au patient concerné un niveau plus élevé de protection des données** s'applique toujours.

En plus de la réglementation nationale HIPAA, des lois supplémentaires sur la protection des données s'appliquent dans certains États, tels que la Californie, New York ou le Texas. Dans la mesure où ces lois ont des exigences plus strictes que l'HIPAA, elles prévalent. Dans ces cas, ONCARE se conformera à la loi applicable la plus stricte.

11. Exercice des droits HIPAA (procédures, vérification d'identité, délais)

Utilisateurs résidant aux États-Unis ou dont les données sont traitées par U.S. Les entités couvertes ont les droits énoncés à l'article 4 de la présente politique de confidentialité conformément à la loi HIPAA.

Les réglementations suivantes s'appliquent à l'exercice de ces droits :

11.1 Champ d'application

Les droits HIPAA peuvent être exercés par :

- demande écrite par e-mail à : **privacy@myoncare.com**
- Demande écrite concernant le prestataire de soins de santé concerné (*Entité visée*)

11.2 Vérification de l'identité

Pour la protection de la personne concernée, toute demande d'exercice des droits ne sera traitée qu'après **vérification réussie de l'identité**. Les mesures possibles sont les suivantes :

- Comparaison avec les données utilisées lors de l'inscription
- Présentation d'une pièce d'identité avec photo valide (en téléchargement sécurisé)
- Confirmation du médecin traitant

11.3 Délais de traitement

ONCARE traite les demandes :

- **dans un délai de 30 jours calendaires** à compter de la date de réception de la demande,
- Extension pour **30 jours supplémentaires** est autorisée une fois ; le demandeur en est informé par écrit et reçoit la justification
- toutes les demandes et réponses seront documentées et archivées conformément au 45 CFR §164.530(j).

12. Traitement des données en dehors des États-Unis (Offshoring / Localisation des données)

Dans certains cas, le traitement des RPS peut être effectué pour le compte d'un fournisseur américain de services de santé. entité visée **en dehors des États-Unis**, en particulier:

- par ONCARE GmbH, établie en Allemagne (UE),
- Fournir des services d'infrastructure technique, d'hébergement, de support et de développement de produits.

Ce traitement transfrontalier est effectué exclusivement :

- sur la base d'un **Contrat de partenariat commercial** (BAA),
- avec une documentation explicite dans le plan de gestion des risques HIPAA de l'entité couverte,
- avec le respect de la règle de sécurité HIPAA ainsi que des **mesures de sécurité selon la norme européenne GDPR**, en particulier:

  → Chiffrement de bout en bout (AES-256),
  → Restriction d'accès selon le principe du besoin d'en connaître,
  → Enregistrement de tous les accès avec piste d'audit,
  → Stockage des données uniquement sur des serveurs avec contrôle d'accès physique et certification ISO 27001.

PHI est **non stocké sur des systèmes en dehors des États-Unis sans mesures techniques de protection appropriées** et la protection contractuelle.

Mesures de protection administratives

ONCARE a mis en œuvre des mesures administratives en vertu de l'article 45 CFR §164.308 pour tous les services liés aux États-Unis, y compris :

- **Délégués à la protection des données et responsables de l'entreprise HIPAA**
- **Politiques de confidentialité et de sécurité**, versionné, documenté et soutenu par une formation
- **Formation obligatoire pour tous les employés** qui travaillent avec des données de santé américaines (au moins une fois par an)
- **Règlement des sanctions** pour les violations de la protection des données telles que définies par 45 CFR §164.530(e)
- **Évaluation des systèmes basée sur les risques et évaluations des vulnérabilités**, au moins une fois par an ou en cas de modifications importantes du système

Tous les processus sont documentés dans un **manuel de conformité HIPAA** interne, qui est régulièrement mis à jour et examiné dans le cadre de l'audit interne.

14. Mesures de sécurité techniques de la règle HIPAA

ONCARE a entièrement mis en œuvre des mesures de protection techniques conformément au 45 CFR §164.312 :

Catégorie	Mesure
Contrôle d'accès	Accès basé sur les rôles, ID utilisateur unique, déconnexion automatique des sessions, procédures d'accès d'urgence
Contrôles d'audit	Enregistrement complet du système et des accès avec évaluation régulière

Catégorie	Mesure
Contrôles d'intégrité	Contrôles d'intégrité basés sur le hachage et contrôle de version pour les données médicales critiques
Authentification	Authentification à deux facteurs pour le personnel médical et les administrateurs
Sécurité du transport	Cryptage TLS 1.3 pendant la transmission, protection VPN pour tous les fournisseurs de services externes

Ces mesures s'appliquent à tous les systèmes qui stockent, traitent ou transmettent des données de santé protégées. La mise en œuvre est assurée annuellement par des tests techniques d'intrusion et une **analyse des risques conforme à la loi HIPAA** .

***