

## PLATEFORME MYONCARE – FOURNISSEUR DE SERVICES DE POLITIQUE DE CONFIDENTIALITE À PARTIR D'OCTOBRE 2025

Bienvenue sur myoncare, le portail de santé numérique pour des soins efficaces et adaptés aux besoins des patients.

Pour nous, chez Oncare GmbH (ci-après dénommée «**ONCARE**» ou «**nous**», «**Nous**», «**notre**»), la protection de votre vie privée et de toutes les données personnelles vous concernant lors de l'utilisation du portail myoncare est d'une grande importance. Nous sommes conscients de la responsabilité qui découle de la mise à disposition et de l'enregistrement de vos données personnelles sur le portail myoncare (= plateforme). 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.

Cette politique de confidentialité se compose de deux parties :

- La première partie contient les règles de protection des données pour l'utilisation de la plateforme myoncare en Europe sur la base du règlement général sur la protection des données (RGPD).
- La deuxième partie contient des dispositions supplémentaires conformément aux exigences de la loi américaine sur la protection des données (HIPAA). Celles-ci s'appliquent en particulier **si les données de santé sont traitées par une entité couverte aux États-Unis ou si les prestataires de services opèrent dans le cadre du système de santé américain** – quel que soit le lieu de résidence de la personne concernée.

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 découvrirez pourquoi et comment **ONCARE** traite vos données personnelles que nous collectons auprès de vous ou que vous nous fournissez lorsque vous décidez d'utiliser le portail myoncare. En particulier, vous trouverez une description du type de données à caractère personnel que nous collectons et traitons, ainsi que la finalité et la base sur lesquelles nous traitons les données à caractère personnel ; En outre, vous trouverez ici les droits auxquels vous avez droit.

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

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

### 1. DÉFINITIONS

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

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

« **Fournisseur de plan de soins** » désigne vous ou tout autre fournisseur de services ou tiers (par exemple, un fabricant de dispositifs médicaux, une société pharmaceutique) qui met des Plans de soins à la disposition d'autres utilisateurs du Portail par le biais de la Boutique myonclinic ou d'autres moyens d'échange de données.

« **Utilisateur du plan de soins** » désigne vous ou un autre prestataire de services (Utilisateur du Portail) qui utilise un Care Plan (« **Pathway** ») pour le traitement de ses Patients Enregistrés.

« **Pathway** » est un plan de traitement standardisé composé de plusieurs CareTasks, 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.

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

« **L'application myoncare** » désigne l'application mobile myoncare pour les patients qui souhaitent utiliser les services proposés par ONCARE par le biais de l'application.

« **Boutique myonclinic** » est la plateforme exploitée par **ONCARE** qui fournit des concepts de soins numériques (plans de traitement) pour le traitement de vos patients enregistrés via le portail myoncare.

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

« **myoncare PWA** » désigne l'application myoncare Progressive Web App pour les patients qui souhaitent utiliser les services proposés par ONCARE via la 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 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 vous ou un autre prestataire de services utilisant le portail Web myoncare.

« **Politique de confidentialité des patients** » désigne la Politique de Confidentialité qui décrit la collecte, l'utilisation et le stockage des informations personnelles (de santé) des Patients utilisant l'Application myoncare. 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.

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

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

### 2. TRAITEMENT DES DONNÉES

Oncare GmbH, une société immatriculée au tribunal d'instance de Munich sous le numéro d'immatriculation 219909 dont le siège social est situé Balanstraße 71a, 81541 Munich, Allemagne, propose et exploite le portail web interactif myoncare Portal (pour les professionnels de la santé) et l'application mobile myoncare App (pour les patients) comme accès aux services myoncare. Cette **politique de confidentialité** s'applique à toutes

les données à caractère personnel traitées par ONCARE dans le cadre de l'utilisation du **portail myoncare**. Pour l'utilisation de l'**application myoncare** par les patients, vous trouverez une politique de confidentialité distincte pour les patients ici: <https://www.myoncare.com/privacy-policy>

### 3. QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

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

**"Données de santé"** désigne les données 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. (au sens de l'art. 4 n° 5 du RGPD).

#### Myoncare PWA

Une Progressive Web App (PWA) est un site Web qui ressemble et possède 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 « 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'appliquent également à l'**application myoncare PWA**, sauf indication contraire dans cette section.

### 4. QUELLES SONT LES DONNÉES PERSONNELLES 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 collectez des données personnelles de vos patients, telles que le nom, l'âge, la taille, le poids, l'indication, les symptômes de la maladie et d'autres informations en rapport avec le traitement de vos patients (par exemple dans le cadre d'un care plan) dans le **portail myoncare**. Les données d'activité de vos patients connectés sont mises à votre disposition dans votre **portail myoncare**.

**Données du magasin commercial** : Données de la Boutique commerciale : Données à caractère personnel traitées dans le cadre de l'utilisation de la Boutique myonclinic – 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. L'utilisation de la boutique myonclinic est facultative et n'est pas nécessaire pour accéder au portail myoncare. Votre utilisation du Portail ne dépend pas du consentement au traitement des données commerciales du Magasin.

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

#### Analyse des données d'utilisation anonymisées pour l'amélioration de la plateforme :

Nous ne traitons que des données techniques d'utilisation anonymes et non personnelles (par exemple, des informations agrégées sur la fréquence d'utilisation ou les performances du système) afin de développer davantage la fonctionnalité et l'expérience utilisateur du portail. Ces données ne contiennent aucune information d'identification et ne permettent pas de tirer des conclusions sur les utilisateurs individuels du portail. Les données personnelles des prestataires de soins de santé ne sont pas traitées à des fins de recherche ou commerciales.

#### Données provenant de fabricants de dispositifs ou de laboratoires :

En outre, les données à caractère personnel peuvent être traitées par des fabricants de dispositifs médicaux connectés 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 dans le cas où vous signalez un incident afin d'assurer la sécurité juridique ou la vigilance des entreprises de dispositifs médicaux ou pharmaceutiques.

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

## 5. TRAITEMENT DES DONNÉES OPÉRATIONNELLES

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

En cas de demande de service, les données personnelles suivantes peuvent également être consultées par les employés autorisés d'ONCARE : Vos données personnelles que vous nous avez fournies pour l'inscription et/ou la connexion à notre portail (par exemple, nom, date de naissance, photo de profil, coordonnées). Les employés autorisés d'ONCARE qui sont autorisés à accéder à votre base de données 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 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** (Progressive Web App) et l' **application myoncare** pour vous informer sur les tâches, les échéances 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 permettra de ne manquer aucune notification importante et de garantir le bon déroulement de votre assistance.

### Pourquoi nous faisons cela :

Notre objectif est de veiller à ce que vous soyez toujours informé de vos tâches et des mises à jour importantes afin de soutenir de manière optimale vos soins.

Les e-mails sont un moyen fiable de s'assurer que des informations importantes vous parviennent, même lorsque les notifications push sont désactivées.

### Vos options d'action :

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

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

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

L'application utilise l'API Google Maps pour utiliser les informations géographiques. Pendant l'utilisation de google Maps, Google collecte, traite et utilise également les données relatives à l'utilisation des fonctions de cartes. Vous trouverez 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 du **portail 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, etc.). En outre, les données personnelles (adresse e-mail) sont traitées dans le cadre de l'authentification à deux facteurs chaque fois que vous vous connectez au **portail myoncare**.

**Justification du traitement :** Le traitement des données 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 le **portail myoncare**.

## 6. 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 patients utilisateurs. 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 pourrait 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 consulter <https://ipapi.com/privacy/> et [Politique de confidentialité |Plateforme de localisation Geoapify](#).

## 7. TRAITEMENT DES DONNÉES (DE TRAITEMENT)

En utilisant le **portail myoncare**, vous saisissez les données personnelles (de santé) de vos patients dans le **portail myoncare** (ex : mise à disposition d'un plan de traitement individualisé, rappel de la prise de médicaments, etc.). De plus, vous et vos patients pouvez télécharger des

documents et des fichiers dans le **portail myoncare** et les partager les uns avec les autres. De plus, des fonctions de localisation peuvent être générées et mises en œuvre :

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

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

Une politique de confidentialité téléchargée sera affichée à chaque patient qui se connecte au site Web. Toutes les déclarations de consentement doivent être documentées dans la politique de confidentialité téléchargée. Une fois qu'une politique de confidentialité a été téléchargée, elle ne peut être remplacée que par une nouvelle version, mais ne peut pas être supprimée.

Les fichiers sont stockés dans une base de données cloud en Allemagne. Vous pouvez autoriser le partage de ces fichiers avec d'autres **utilisateurs du portail** au sein de votre établissement à des fins médicales. Les autres **utilisateurs du portail** n'ont pas accès à ces fichiers.

Vous pouvez également consulter un prestataire extérieur à votre établissement (médecin consultant) dans le cadre de la prise en charge de vos patients, si vous estimez qu'un autre avis d'expert sert au traitement.

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

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

## 8. TRAITEMENT DES DONNÉES TECHNIQUES D'UTILISATION ET DU SYSTÈME

**Ne s'applique que si vous utilisez le myonclinic Store en tant qu'utilisateur de Careplan.**

Le **myonclinic store** est intégré dans le **portail myoncare** et propose l'achat de plans de traitement (Careplan). Après vous être inscrit dans le **portail myoncare**, vous pouvez vous connecter au **myonclinic store** avec vos données de connexion. Vous pouvez utiliser le **myonclinic store** pour acheter des plans de traitement en tant qu'utilisateur.

**Données de l'utilisateur du Careplan :**

Les données des **Utilisateurs du Careplan**, que le **myonclinic Store** traite pendant l'utilisation, sont traitées dans le but de conclure un contrat de licence avec le **Fournisseur de Careplan** – dans ce cas ONCARE – et, si des frais sont dus, pour le traitement et le contrôle du processus de paiement entre le **Fournisseur de Careplan** – en l'occurrence ONCARE – et les **Utilisateurs du Careplan**.

**Types de données:** nom, coordonnées, coordonnées bancaires.

**Traitement des données du store commercial :** Données à caractère personnel que nous traitons lors de l'utilisation du **myonclinic store** dans le cadre de l'achat de plans de traitement. En outre, les données de paiement (si des frais d'utilisation sont facturés) seront **transmises au fournisseur de Careplan**.

**Justification du traitement des données des magasins commerciaux :** La base juridique du traitement des données du store commercial est l'art. 6 (1) (b) du RGPD – le traitement des données sert à l'exécution du contrat entre l'**utilisateur Careplan** et le **fournisseur de Careplan** – dans ce cas, ONCARE.

## 9. TRAITEMENT DES DONNÉES D'ACTIVITÉ

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

Les **outils myoncare** offrent aux **utilisateurs de l'application** la possibilité de connecter l'**application myoncare** à certaines applications de santé (par exemple AppleHealth, GoogleFit, Withings) ("**Application Santé**"), à condition que ceux-ci soient utilisés par les **utilisateurs de l'application** et la connexion est établie par l'**utilisateur de l'application**. Une fois connectés, les données d'activité collectées par l'**Application Santé** seront mis à votre disposition pour vous fournir des informations contextuelles supplémentaires concernant l'activité de l'**utilisateur de l'application**. Veuillez noter que les données d'activité **ne sont pas originales** des outils myoncare et ne doivent donc pas être utilisées à des fins de diagnostic comme base de décisions médicales.

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

**Types de données :** Le type et l'étendue des données transférées dépendent de la décision des **utilisateurs de l'application**. Les données comprennent le poids, la taille, les pas effectués, les calories brûlées, les heures de sommeil, la fréquence cardiaque et la pression artérielle, entre autres.

**Finalité du traitement des données d'activité :** Les données d'activité de l'Utilisateur de l'application **Données d'activité** vous est fournie afin de vous fournir des informations contextuelles supplémentaires concernant l'activité de l'**utilisateur de l'application**. Veuillez noter que les données d'activité ne sont pas validées par les **outils myoncare** et ne doivent pas être utilisées à des fins diagnostiques ou comme base de décisions médicales.

**Raison du traitement :**

Le responsable de traitement est le patient lui-même, en vous donnant accès à ses données d'activité afin de vérifier les informations partagées. Il n'y a donc pas besoin d'une justification supplémentaire.

## 10. TRAITEMENT DES DONNÉES RELATIVES À LA SÉCURITÉ DES PRODUITS

Ne s'applique que si vous utilisez la variante dispositif médical des outils myoncare.

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

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

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

**Traitement des données de sécurité des produits:** Nous stockons et évaluons toutes les données à caractère personnel dans le cadre de nos obligations légales en tant que fabricant d'un dispositif médical et transmettons ces données à caractère personnel (dans la mesure du possible après pseudonymisation) aux autorités compétentes, aux organismes notifiés ou à d'autres responsables du traitement des données ayant des obligations de surveillance. En outre, nous stockons et transférons des données personnelles relatives aux dispositifs médicaux et/ou aux médicaments lorsque nous recevons des communications de votre part en tant que rapporteur de ces informations, de votre 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 personnelles pour l'exécution d'obligations légales en tant que fabricant de dispositifs médicaux ou de médicaments 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.

## 11. TRAITEMENT PAR LES FABRICANTS D'ÉQUIPEMENTS 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 tiers externes (par exemple, des fabricants de dispositifs médicaux 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.

## 12. GESTION DES DONNÉES COMMERCIAUX ET DES PATHWAYS

Le portail myoncare offre aux prestataires de services enregistrés (par exemple des médecins) la possibilité de proposer et de configurer des care pathways 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'assignation d'un pathway. Ce traitement des données sert à l'individualisation et à l'assignation 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.

## 13. TRAITEMENT DES DONNÉES DE REMBOURSEMENT EN CAS DE TRANSMISSION DE L'OBJET DE LA REDEVANCE

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

Le **portail myoncare** vous accompagne dans l'initiation de vos procédures standards de remboursement des prestations de santé que vous avez fournies à vos patients via L'**application myoncare**. Pour permettre le processus de remboursement, le **portail myoncare** prend en charge la collecte des données personnelles (liées à la santé) de vos patients à partir du **portail myoncare** afin de faciliter la transmission de ces données aux payeurs du patient dans le cadre des processus de remboursement habituels (soit votre association des médecins de l'assurance maladie obligatoire, soit la caisse d'assurance maladie du patient). Vous êtes le responsable du traitement des données de remboursement et êtes responsable du respect des réglementations en matière de protection des données pour le traitement des données personnelles de vos patients dans le cadre du processus de remboursement. ONCARE agit en tant que sous-traitant des données sur la base de l'accord de traitement des données conclu avec le **Fournisseur de services**.



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

**Traitement des données de remboursement:** En tant que responsable du traitement, vous transmettez les données de traitement du patient nécessaires au remboursement au payeur (soit votre caisse d'assurance maladie et/ou la compagnie d'assurance maladie du patient) et le payeur traite les données de remboursement afin de vous rembourser.

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

#### 14. 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 d'une version à jour 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 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 ;
- Remplacez les notifications push par des e-mails pour **PWA** (Progressive Web App) dans les cas suivants :
  - Si un care plan se termine dans la journée ;
  - 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.

##### 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.

##### Brevo (Politique de confidentialité) :

[Politique de confidentialité - Protection des données personnelles | Brevo](#)

##### SendGrid

<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 :

- Le système d'exploitation de l'utilisateur ;
- Géolocalisation de l'utilisateur ;
- Navigateur;
- Rôle;
- Adresse IP;
- Sites Web visités via le Web/PWA (voir la section sur les PWA dans la présente politique de confidentialité pour plus d'informations) ;
- Les boutons sur lesquels l'utilisateur clique dans le **portail myoncare**, dans l' **application myoncare** et dans 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 des utilisateurs. 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.

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

## 16. TRANSFERTS DES DONNÉES / DIVULGATION À DES TIERS

Vos données personnelles ne seront transmises à des tiers que dans le cadre des dispositions légales ou sur la base de votre consentement. Dans tous les autres cas, les informations ne seront pas divulguées à des tiers, sauf si nous y sommes obligés en raison de dispositions légales impératives (divulgaration 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.

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

## 17. 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, le **portail myoncare** vous en informera expressément dans le cadre de la procédure de consentement.

Traitement de catégories particulières de données à caractère personnel conformément à l'Art. 9 (1) du RGPD ne peut avoir lieu que si cela est nécessaire en raison de dispositions légales et qu'il n'y a aucune raison de supposer que vos intérêts légitimes s'opposent au traitement de ces données à caractère personnel ou que vous avez donné votre consentement au traitement de ces données à caractère personnel conformément à l'art. 9 (2) du RGPD.

Pour le traitement des données pour lequel votre consentement est requis (comme expliqué dans le présent **Politique de confidentialité**), le consentement sera obtenu dans le cadre du processus d'inscription. Une fois l'inscription réussie, les consentements peuvent être gérés dans les paramètres du compte du **portail myoncare**. En outre, ONCARE vous demandera d'accepter un accord de traitement des données pour les données traitées par ONCARE sous votre responsabilité en tant que responsable du traitement. Les consentements requis pour les fonctionnalités supplémentaires facultatives (par exemple, l'utilisation du Store, les données d'activité, les analyses Matomo) sont volontaires. Votre utilisation du portail myoncare ne dépend pas de l'octroi de tels consentements.

## 18. DESTINATAIRES DES DONNÉES / CATÉGORIES DE DESTINATAIRES

Dans le cadre de notre organisation, nous veillons à ce que seules les personnes qui sont tenues de le faire pour remplir leurs obligations contractuelles et légales soient autorisées à traiter des données à caractère personnel.

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

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 de le **portail myoncare**, où sont stockées à la fois vos données personnelles et celles de vos patients. Il héberge également le service de gestion de vidéos et de fichiers de myoncare, qui permet des vidéoconférences cryptées et le partage de données entre vous et votre patient. L'accès à vos données personnelles par vous et votre patient est assuré par l'envoi de tokens spécifiques. Ces données personnelles sont cryptées lors de la transmission et pseudonymisées pour ONCARE et ses prestataires de services lors de la transmission et au repos. 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 du traitement des demandes de service ont été formés en conséquence. À la réception de votre demande de service, un numéro de ticket vous sera assigné.

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. Il s'agit d'une plateforme d'expérience client permettant de gérer les commentaires externes avec la capacité pour 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 une publication Instagram liée, 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>

## 19. 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 le **portail myoncare** ou l'**application myoncare** ne sont pas stockées dans app stores. 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 du **portail myoncare** avec l'**application myoncare** se déroule à l'aide de Google Firebase. Les serveurs de Google Firebase sont hébergés dans l'Union européenne. Néanmoins, conformément aux conditions générales de Google Firebase, un transfert temporaire de données vers des pays dans lesquels Google et les fournisseurs de services associés ont des succursales. 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 non autorisé à vos données est empêché par le chiffrement de bout en bout et par les jetons d'accès sécurisé. Nos serveurs en ligne sont hébergés en Allemagne. À des fins d'analyse, les e-mails envoyés avec SendGrid contiennent ce que l'on appelle un « pixel de suivi » qui se connecte aux serveurs de Sendgrid lors de l'ouverture de l'e-mail. Cela peut être utilisé pour déterminer si un e-mail a été ouvert.

### Base légale

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

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

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.

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. Les **outils myoncare** utilisent ces interfaces, qui sont fournies par Google, Apple et Withings, pour demander des données d'activité aux applications de santé connectées. La demande envoyée par les **les outils myoncare** ne contient aucune donnée personnelle. Les données personnelles sont mises à la disposition des **outils myoncare** via ces interfaces.

## 20. DURÉE DE CONSERVATION DES DONNÉES PERSONNELLES

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

Veuillez noter qu'ONCARE est également soumise à des obligations de conservation convenues contractuellement avec vous sur la base de dispositions légales. De plus, en raison de la classification et, le cas échéant, de votre utilisation du **portail myoncare** et de l'**application MyonCare** en tant que dispositif médical, certaines durées de conservation s'appliquent au portail, qui résultent de la loi sur les dispositifs médicaux. 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.



## 21. VOS DROITS EN TANT QUE PERSONNE CONCERNÉE

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

Dans certains cas, les données personnelles doivent également être collectées ou mises à disposition conformément 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.

## 22. DÉCISIONS AUTOMATISÉES DANS DES CAS INDIVIDUELS

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

## 23. 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, d'effacement et d'opposition. Vous avez également le droit de recevoir une copie de toutes les données personnelles que nous détenons à votre sujet.

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

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

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

**Droit à la limitation du traitement des données (Art. 18 du RGPD) :** Vous avez le droit de demander la limitation du traitement de vos données à caractère personnel si l'exactitude des données est contestée, si le traitement est illégal, si les données sont nécessaires 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.

Pour exercer ces droits, veuillez nous contacter à l'adresse suivante : [privacy@myoncare.com](mailto:privacy@myoncare.com). L'opposition et la révocation du consentement doivent être soumises à [privacy@myoncare.com](mailto:privacy@myoncare.com) sous forme de texte.

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](mailto: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.

## 24. 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](mailto:privacy@myoncare.com).

## 25. SOUS RÉSERVE DES MODIFICATIONS APPORTÉES À LA PRÉSENTE 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.

Des modifications sont possibles à tout moment et vous seront notifiées de manière appropriée et dans un délai raisonnable avant leur date d'entrée en vigueur (par exemple, en publiant une **politique de confidentialité** révisée lors de la connexion ou en fournissant un préavis des changements importants).

ONCARE GmbH Adresse postale : Balanstraße 71a, 81541 Munich, Allemagne

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

Coordonnées du délégué à la protection des données [privacy@myoncare.com](mailto:privacy@myoncare.com)

Si des contenus ou des services médicaux sont obtenus ou proposés via la boutique intégrée myonclinic, le contenu et la responsabilité économique sont assumés par myon.clinic GmbH, une filiale d'Oncare GmbH. Dans ce contexte, Oncare GmbH ne fournit que la plate-forme technique. [privacy@myon.clinic](mailto:privacy@myon.clinic)

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

\* \* \*

Ce qui suit **sont des réglementations complémentaires en matière de protection des données pour les prestataires de services** qui agissent en tant qu'entité visée **dans** États-Unis d'Amérique **dans le cadre de** une activité conforme à la loi HIPAA **ou au nom d'une telle entité**:

La protection des informations personnelles de santé (PHI) en vertu de la loi HIPAA ne s'applique que si ces données sont traitées dans le cadre des États-Unis, système de soins de santé par une entité dite couverte ou un partenaire commercial – indépendamment de la nationalité ou du domicile de la personne concernée. Le seul facteur décisif est que le traitement entre dans le champ d'application de la loi HIPAA.

## **us Réglementations supplémentaires sur la protection des données pour les fournisseurs de services aux États-Unis d'Amérique (HIPAA)**

### **1. Champ d'application**

Le présent addendum HIPAA s'applique à tous les fournisseurs de services qui traitent, stockent ou partagent des informations de santé protégées (PHI) par le biais de la plateforme ONCARE, à condition que ce traitement soit en relation avec un sous-traitant réglementé par la HIPAA (« entité couverte ») ou qu'ONCARE agisse en tant que partenaire commercial.

### **2. Rôles et responsabilités**

ONCARE agit en tant que partenaire commercial en vertu de la règle de confidentialité HIPAA (45 CFR §160.103) et s'engage à se conformer à toutes les réglementations HIPAA applicables à l'entité couverte. Le prestataire de services concerné agit soit :

- en tant que membre du personnel de l'entité couverte, ou
- en tant que sous-traitant d'ONCARE conformément au 45 CFR §160.103 et suivants.

### **3. Châssis d'usage**

L'utilisation de la plateforme ONCARE par les fournisseurs de services est uniquement basée sur des accords existants conformes à la loi HIPAA avec l'entité couverte (par exemple, des accords de partenariat commercial ou des accords de fournisseur de services). Le traitement comprend notamment :

- Documentation des traitements et des prestations médicales,
- Communiquer avec les patients à l'aide de canaux de communication conformes à la loi HIPAA (cryptage de bout en bout, TLS)
- Accès aux données structurées des patients pour les soins ou l'assurance qualité.

L'utilisation de la plateforme ONCARE par les prestataires de soins de santé n'est pas subordonnée à un consentement supplémentaire (autorisation) pour les activités de traitement facultatives. Tous les traitements de données nécessaires aux soins sont basés sur la loi HIPAA et les accords respectifs.

### **4. Confidentialité et contrôle d'accès**

Les fournisseurs s'engagent à préserver la confidentialité de tous les RPS et à limiter l'accès aux RPS dans la mesure nécessaire, conformément à la norme minimale nécessaire (45 CFR §164.502(b)). Chaque accès est géré via un concept de droits basé sur les rôles et enregistré de manière vérifiable.

### **5. Mesures de sécurité techniques et organisationnelles**

Toutes les mesures de sécurité mises en œuvre par ONCARE sont conformes aux exigences de la règle de sécurité HIPAA (45 CFR Part 164, Subpart C). Il s'agit notamment de :

- Cryptage AES-256 des données stockées,
- transmission cryptée via TLS 1.3,
- Authentification à deux facteurs (2FA),
- analyses périodiques des risques conformément à l'article 164.308(a)(1)(ii)(A),
- des processus structurés de réponse aux incidents.

### **6. Traitement des données en dehors des États-Unis**

Lorsque les fournisseurs accèdent à des données par l'intermédiaire d'ONCARE qui sont traitées ou stockées en dehors des États-Unis (par exemple, l'hébergement dans l'UE), ils le font exclusivement :

- sur la base d'une protection contractuelle conforme à la loi HIPAA (par exemple BAA de sous-traitant),
- avec le consentement documenté de l'Entité couverte,
- dans le respect de la règle de sécurité HIPAA et des normes internationales complémentaires (par ex. B. ISO 27001, principes du RGPD),

- et avec un cryptage et un contrôle d'accès de bout en bout.

## 7. Obligations de signalement en cas d'incidents relatifs à la protection des données

Les fournisseurs sont tenus d'informer immédiatement ONCARE de tout incident qui pourrait entraîner un accès non autorisé aux RPS (« incident de sécurité » ou « violation » telle que définie dans 45 CFR §164.304/§164.402). ONCARE se charge de la coordination des rapports légalement requis à l'intention de l'entité couverte et des personnes concernées.

## 8. Droits de l'entité visée

L'Entité visée se réserve le droit, à tout moment, d'auditer l'accès, l'utilisation et les mesures de sécurité concernant les RPS par ONCARE et les Fournisseurs de services associés. Les prestataires de services doivent assurer une coopération totale.

## 9. Pas de distribution indépendante

Le Prestataire de services ne peut divulguer des RPS à des tiers en dehors de la Plateforme (par exemple, par e-mail, système externe, impression) que si :

- il existe une « autorisation » documentée de la part de la personne concernée ou
- Cela est expressément prévu dans le contrat.

## 10. Préséance et interprétation

En cas de conflit entre le présent supplément HIPAA et les règles européennes de protection des données, la règle la plus stricte s'appliquera toujours, à condition qu'elle soit conforme à la loi applicable. États-Unis les lois fédérales sur la protection de la vie privée (par exemple, CCPA) restent inchangées et les lois étatiques sur la protection de la vie privée ne sont pas affectées et s'appliquent en plus le cas échéant.

## 11. Soutien aux droits des personnes concernées

Les prestataires de services aident ONCARE et l'entité couverte concernée à respecter les droits des personnes concernées conformément à 45 CFR §§ 164.524-528 (par exemple, information, correction, restriction de la divulgation). Cela inclut notamment la participation à :

- la mise à disposition de journaux d'accès (« Accounting of Disclosures »),
- la correction de DAP erronés,
- la mise en œuvre d'avis de blocage ou de restrictions d'utilisation.

Les demandes seront coordonnées par ONCARE et traitées avec un préavis de 30 jours, avec une prolongation possible de 30 jours supplémentaires sur notification.

## 12. Obligation de dispenser une formation à la protection des données

Les prestataires de services sont tenus d'organiser chaque année une formation documentée sur les exigences en matière de protection des données selon HIPAA et GDPR.

À cet effet, ONCARE met à disposition du matériel adapté ou un accès à l'apprentissage en ligne. La participation est documentée numériquement et doit être prouvée à l'entité couverte sur demande.

## 13. Utilisation secondaire et données de recherche

Toute utilisation des PHI à des fins de recherche, d'analyse ou de marketing par le fournisseur de soins de santé est interdite. À des fins de recherche et d'analyse, ONCARE n'utilise que des données anonymisées telles que définies dans 45 CFR §164.514. Étant donné que ces données ne sont plus considérées comme des RPS, aucune autorisation n'est requise. Toute utilisation secondaire interne (par exemple, pour l'assurance qualité) est autorisée uniquement dans le cadre de la limitation de l'objectif en vertu de la loi HIPAA.

## 14. Coordination avec les exigences du RGPD

Grâce à l'applicabilité simultanée du RGPD et de l'HIPAA, ONCARE veille à ce que le niveau de protection le plus strict s'applique toujours. En particulier, les prestataires s'engagent à :

- ne pas transférer de données en dehors de l'EEE sans clauses contractuelles types ou sous-BAA appropriées ;
- Coordonner les droits des personnes concernées des deux juridictions (par exemple, le droit à l'effacement en vertu de l'art. 17 du RGPD par rapport aux obligations de conservation en vertu de la loi HIPAA) conformément à ONCARE.

## 15. Exigences supplémentaires de l'État en matière de protection des données (États-Unis)

En plus des réglementations fédérales en vertu de la loi HIPAA (Health Insurance Portability and Accountability Act), certains traitements de données sont soumis à des lois supplémentaires ou plus strictes sur la protection des données de chaque État américain. Cela s'applique en particulier si les utilisateurs concernés résident dans l'un de ces États, utilisent nos services à partir de là ou si les données personnelles sont traitées par des prestataires de services ou des partenaires contractuels basés dans ces États.

Les lois fédérales suivantes sur la protection de la vie privée peuvent être appliquées en plus ou en priorité, selon la constellation individuelle :

- Californie : California Consumer Privacy Act (CCPA) et California Privacy Rights Act (CPRA)
- New York : Loi SHIELD
- Virginie : Loi sur la protection des données des consommateurs de Virginie (VCDPA)
- Colorado : Loi sur la protection de la vie privée du Colorado (CPA)
- Connecticut : Loi sur la confidentialité des données (CTDPA)
- Utah : Loi sur la protection de la vie privée des consommateurs de l'Utah (UCPA)
- Illinois : Loi sur la confidentialité des informations biométriques (BIPA)

- Texas : Loi sur la confidentialité et la sécurité des données (TDPSA, en vigueur le 01.07.2024)
- Floride : Déclaration des droits numériques (FDBR)

Nous nous engageons à respecter les réglementations fédérales applicables pour toutes les activités de traitement et à fournir aux personnes concernées des informations complètes sur l'application de ces droits sur demande. Pour certains États (par exemple, la Californie), nous fournissons des avis de confidentialité distincts sur demande. Veuillez nous contacter à l'adresse suivante : [privacy@myoncare.com](mailto:privacy@myoncare.com) si vous souhaitez exercer vos droits relatifs à la vie privée en vertu de la loi fédérale ou étatique.

#### 16. Aucune utilisation commerciale des données personnelles de l'utilisateur du portail

Les données personnelles des utilisateurs du portail (par exemple, les prestataires de soins de santé) ne sont pas utilisées à des fins de recherche, de marketing ou à d'autres fins commerciales. ONCARE ne traite que des données d'utilisation techniques entièrement anonymisées (par exemple, des horodatages de connexion agrégés ou des modèles d'utilisation du système) afin d'améliorer les performances techniques de la plateforme. Ces données ne contiennent aucune information qui pourrait être utilisée pour identifier des utilisateurs individuels et ne sont pas considérées comme des informations de santé protégées (PHI) en vertu de la règle de confidentialité HIPAA.

\*\*\*