MYONCARE PATIENT APP – PRIVACY POLICY (EUROPE/USA)

AS OF JUNE 2025

Welcome to myoncare, the digital health portal and mobile app ("**App**") for efficient and needs-based patient care and support for occupational health management.

This privacy policy is divided into two parts:

- The first part contains the data protection regulations for the use of the myoncare platform within Europe in compliance with the **EU General Data Protection Regulation (GDPR).**

- The second part contains **additional information** in accordance with the requirements of **the United States of America Data Protection Law (HIPAA),** in particular for users residing in the USA or in the case of processing of health data by US healthcare providers.

For us at Oncare GmbH (hereinafter referred to as "**ONCARE"** or "**we**", **"we**", "**our**"), the protection of your privacy and any personal data relating to you while using the **App** is of great importance and importance. We are aware of the responsibility that arises from your trust in the provision and storage of your personal (health) data in the myoncare app. Therefore, our technology systems used for the myoncare services are set up to the highest standards and the lawful processing of the data is at the heart of our ethical understanding as a company.

We process your personal data in accordance with applicable legislation on the protection of personal data, in particular the EU General Data Protection Regulation ("**GDPR")** and the country-specific laws that apply to us. In this privacy policy, you will learn why and how **ONCARE** processes your personal (health) data that we collect from you or that you provide to us when you decide to use the myoncare app. In particular, you will find a description of the personal data we collect and process, as well as the purpose and basis on which we process the personal data and the rights to which you are entitled.

Please read the Privacy Policy carefully to ensure that you understand each provision. After reading the Privacy Policy, you will have the opportunity to agree to the Privacy Policy and consent to the processing of your personal (health) data as described in the Privacy Policy. If you give your consent, the Privacy Policy becomes part of the contract between you and Oncare.
According to the terms of use, our offer is only aimed at persons aged 18 and over. Accordingly, no personal data of children and adolescents under the age of 18 is stored and processed.

1. DEFINITIONS

"**App User**" means any user of the myoncare App (Patient and/or Employee).

"**Blockchain**" is another database in the myoncare system that stores corresponding data of the application.

"**Company**" means your employer if you and your employer use myoncare tools for the employer's occupational health management.

"**Data Service Provider**" means any agent engaged and instructed by the Company to collect, review and interpret pseudonymized or anonymized employee data in occupational health management programs on the basis of a separate service agreement with the Company (e.g., data analyst, general health prevention services, data evaluation services, etc.), which is provided by a separate information sheet to employees.

"**Healthcare Provider**" means your physician, clinic, healthcare facility, or other healthcare professional acting alone or on behalf of your physician, clinic, or healthcare facility.

"Pathway" is a standardised treatment plan consisting of several care tasks, possibly sequenced together in time, which can determine the steps for diagnoses and therapies.

"Care tasks" are specific tasks or actions within a pathway that must be performed by the healthcare providers involved, the nursing staff or the patient himself.

"**myoncare App**" means the mobile myoncare application for use by patients or employees who wish to use the services offered by ONCARE.

"**myoncare Portal**" is the myoncare web portal, which is intended for professional use by portal users and serves as an interface between portal users and app users.

"**myoncare Tools**" means the myoncare app and the myoncare portal together.

"**myoncare PWA** " means the myoncare Progressive Web App application for patients who wish to use the services offered by ONCARE through the PWA and not through the myoncare App.

"**myoncare Services**" means the services, functionalities and other offers that are or may be offered to Portal Users via the myoncare Portal and/or to App Users via the myoncare App.

"**ONCARE"** means ONCARE GmbH, Germany.

"**Portal User**" means any healthcare provider, company or data service provider using the web-based myoncare Portal.

"**Privacy Policy**" means this statement given to you as a patient and user of the myoncare App, which describes how we collect, use and store your personal information and informs you of your broad rights.

"**Terms of Use**" means the terms of use for the use of the myoncare App.

2. PROCESSING OF (TREATMENT) DATA

Oncare GmbH, a company registered with the District Court of Munich under registration number 219909 with its registered office at Balanstraße 71a, 81541 Munich, Germany, offers the **mobile application myoncare App** and operates it as access to the **myoncare Services**. This **privacy policy** applies to all personal data processed by ONCARE in connection with the use of the **myoncare app** .

3. WHAT IS PERSONAL DATA

"**personal data**" means any information that allows a natural person to be identified. In particular, this includes your name, birthday, address, telephone number, email address and IP address.

"**Health data**" means personal data relating to the physical and mental health of a natural person, including the provision of health services that disclose information about their health status.

Data is to be considered "**anonymous**" if no personal connection to the person/user can be established.
In contrast, "**pseudonymized**" data is data from which a personal reference or personally identifiable information is replaced by one or more artificial identifiers or pseudonyms, but which can generally be re-identified by the identifier key.

4. myoncare PWA

A Progressive Web App (PWA) is a website that looks and has the functionality of a mobile app. PWAs are built to take advantage of the native capabilities of mobile devices without the need for an app store. The goal of PWAs is to combine the difference between apps and the traditional web by bringing the benefits of native mobile apps to the browser. The PWA is based on the technology of "React". "React" is an open source software for PWA applications.

To use the **myoncare PWA** function, patients need a computer or smartphone and an active internet connection. There is no need to download an app.

The following information about the **myoncare app** also applies to the **myoncare PWA**, unless otherwise described in this section.

5. WHAT PERSONAL DATA IS USED WHEN USING THE MYONCARE APP

We may process the following categories of data about you when using the **myoncare app** :

Operational data: Personal data that you provide to us when registering in our **myoncare app**, contacting us about problems with the app or otherwise interacting with us for the purpose of using the app**.**

Treatment data: You or your healthcare provider provide us with your personal data such as name, age, height, weight, indication, disease symptoms and other information related to your treatment (e.g. in a care plan). Information related to your treatment includes, but is not limited to: information about medications taken, responses to questionnaires including disease- or condition-related information, diagnoses and therapies provided by your **healthcare provider** , planned and completed tasks.

Commercial Store Data: Commercial Store Data: Personal data processed in connection with the use of the myoncare Store – in particular in connection with the authorship, configuration or purchase of digital treatment plans ("Pathways"). The store is operated by myon.clinic GmbH, a subsidiary of Oncare GmbH. The use of the Store requires the processing of your name, professional contact details and, if applicable, payment data (only for paid content). Oncare GmbH processes this data exclusively for the technical provision of the platform functions and not for its own commercial purposes.

Activity data: Personal data that is processed by us if you connect the **myoncare app** to a health application (e.g. GoogleFit, AppleHealth, Withings). Your activity data will be transferred to your affiliated **service providers** as **portal users** .

Commercial and non-commercial research data:
We process your personal data in anonymized/pseudonymized form in order to analyze and produce summary scientific reports in order to improve products, treatments and scientific results.

Use of anonymised data for commercial purposes: In addition, ONCARE may use certain health and usage data, once fully anonymised, for commercial purposes – such as improving the platform, analysing care processes, or developing new digital health services. Anonymisation is performed in such a way that individuals can no longer be identified. These anonymised data are therefore no longer subject to the GDPR.

Data from device manufacturers, medical device distributors or laboratories:
In addition, personal data may be processed by connected medical device manufacturers, distributors of medical devices or laboratory service providers as part of integrated care processes, provided that they are commissioned or used by the service provider via the myoncare portal.

Product safety data: Personal data that is processed to comply with our legal obligations as the manufacturer of the **myoncare app** as a medical device. In addition, your personal data may be processed by medical device or pharmaceutical companies to fulfil legal security or vigilance purposes.

Reimbursement Data: Personal data required for the reimbursement process between your provider and your health insurance provider.

Occupational health management data: Personal or aggregated data collected in specific projects and questionnaires at the request of your **company** (either directly or through a data service provider contracted by your company). The data may relate to certain health information, your opinion about your personal well-being, your opinion as an employee on a particular internal or external situation, or data about care or health in general.

6. BLOCKCHAIN TECHNOLOGY

Blockchain **technology** ("**Blockchain**") (European Patent No. 4 002 787) is an optional service that is not mandatory. It is your **service provider** who decides to use the blockchain solution. The **blockchain** is based on Hyperledger Fabric's technology. Hyperledger Fabric is an open-source software for enterprise-level blockchain implementations. It offers a scalable and secure platform that supports blockchain projects.

The blockchain in the myoncare system is an additional database in which data from the application is stored. All blockchain data is stored in the Federal Republic of Germany. It is a private **blockchain** ("**Private Blockchain**"), it only allows the input of selected verified participants and it is possible to overwrite, edit or delete entries as needed.

Generally, the **blockchain** consists of digital data in a chain of packets called "blocks" that store the corresponding transactions. The way these blocks are connected to each other is chronological. The first block that is created is called the genesis block, and each block added after that has a cryptographic hash related to the previous block, so transactions and information changes can be traced back to the genesis block. All transactions within the blocks are validated and verified through a blockchain consensus mechanism to ensure that each transaction remains unchanged.

Each block contains the list of transactions, a timestamp, its own hash, and the hash of the previous block. A hash is a function that converts digital data into an alphanumeric chain. If an unauthorized person tries to change the data of a single block, the hash of the block will also change and the link to that block will be lost. In this case, the block can no longer be synchronized with the others. This technical process prevents unauthorized persons from manipulating the contents of the **blockchain** chain. When all nodes (network nodes) try to synchronize their copies, it detects that a copy has been modified, and the network considers that node to be unhealthy.

Our **blockchain** is a private **blockchain**. A private **blockchain** is decentralized. This is a so-called distributed ledger system that acts as a closed database. Unlike public **blockchains**, which are "unauthorized," private **blockchains** are "authorized" because authorization is required to become a user. Unlike public **blockchains**, which are publicly accessible to everyone, access to private **blockchains** is dependent on eligibility to become a user. This structure makes it possible to take advantage of the security and immutability of blockchain technology while being compliant with data protection and, in particular, complying with the regulations of the General Data Protection Regulation (GDPR). Private blockchain records can be edited, modified, or deleted. In this context, deletion means that the reference value to the UUID (Universally Unique Identifier) in the service **provider's** database is deleted. In addition, the hash is anonymized in the blockchain database, so that this overall process is compliant with the General Data Protection Regulation and the rights of a data subject are guaranteed (right to erasure/"right to be forgotten", Art. 17 GDPR).

Type of data stored and processed in the blockchain:

- Institutions/**Leistungserbinger** UUID
- Patient UUID
- Asset UUID
- Hash of caretask and asset data. (UUID: Universal Unique Identifier).

The files stored in the **blockchain** are pseudo-anonymized.

Our **blockchain** is designed to ensure data privacy in terms of data integrity, patient profile, assets, and assigned **care tasks** and medications. To communicate with the **blockchain**, the user must register a series of public-private keys. To communicate with the **blockchain**, the user needs several public-private keys; the registration process generates certificates that are stored in a separate database of the **provider** and on the patient's mobile phone. A backup copy of the patient key is encrypted and stored in the **provider**'s database , which can only be accessed by the patient.

When verifying consent to data protection, in the event that the **Provider** wants to communicate with the Patient, the system checks whether the Patient has given consent to the Provider's Privacy Policy . The **blockchain** therefore serves to ensure the integrity and accountability of the record to ensure that the patient has accepted the privacy policy.

When a **healthcare provider** uploads a new version of a privacy policy, the hash of the file is stored on the **blockchain** and after the patient gives consent, that interaction is stored on the **blockchain** . Every time the patient communicates, the **blockchain** responds by comparing the hash with a flag that indicates whether the patient's consent is still valid for the current privacy policy.

The integrity of the patient profile is also ensured by the blockchain in patient synchronization . The **healthcare provider** immediately detects if the patient profile is not synchronized or matches the profile on the mobile phone by comparing the hash of the patient profile in the **blockchain**. In this way, the **service provider achieves** sufficient up-to-dateness with regard to the patient profile.

myoncare Portal:
If the **service provider** chooses the blockchain solution, ONCARE implements an additional tool, called "Adapter Service", which is used to communicate with the **blockchain** . The blockchain instance is hosted by ONCARE.

myoncare app:
Patients can connect to the same blockchain instance using the Phone Manager tool, which is also hosted by ONCARE. This service is also hosted by ONCARE.

Legal basis for data processing: Data processing by ONCARE on behalf of the **Service Provider** is carried out on the basis of Art. 28 GDPR (Data Processing Agreement).

7. PROCESSING OF OPERATIONAL DATA

Applicable to all app users

You may provide us with certain personal data when you contact us to understand the functions and use of the **myoncare app** , in the event of a service request from you or in the case of a support offer initiated by us (by telephone).

Service Employees

On behalf of the data controller (e.g. We offer you support in filling out questionnaires by telephone (outbound calls) in order to optimize your digital patient care. If you do not want to take advantage of this offer, you are free not to accept it and to object to telephone support.

In the event of a service request and an outbound call, the following personal data can also be viewed by authorized ONCARE employees:

- The personal data that you have provided to your **service provider** via our app (e.g. name, date of birth, profile picture, contact details).
- The health data that you have provided to your **healthcare provider,** data **service provider** or **employer** via our **myoncare app** (e.g. information about medications taken, responses to questionnaires including disease- or condition-related information, diagnoses and therapies of healthcare professionals, planned and completed tasks).

Authorized ONCARE employees who may access the database of your service provider**,** data service provider **or** employer **for the purpose of processing a service request or an outbound call** are contractually obliged to keep all personal data strictly confidential.

Push notifications and emails
As part of your support from myoncare, we would like to inform you about how we handle notifications and important information that we send you.

1. **Push notifications**:
   - We send you push notifications via our **myoncare PWA** (Progressive WebApp) and **the myoncare app** to inform you about tasks, appointments and important updates.
   - You have the option to disable these push notifications in your app's settings.
2. **Email notifications**:
   - Whether you have enabled or disabled push notifications, we will continue to send you important information and reminders via email.
   - This ensures that you don't miss any important notifications and that your support runs smoothly.

Why we do this:

- Our goal is to keep you up to date with your tasks and important updates to support your health in the best possible way.
- Emails are a reliable way to ensure that important information reaches you, even when push notifications are disabled.

Your options for action:

- If you do not want to receive push notifications, you can deactivate them in the settings of the myoncare app.
- Please ensure that your email address is accurate and up-to-date to ensure a smooth reception of our messages.
- If you do not want to receive email reminders, you can deactivate them in the settings of the myoncare app.

Storage period
The data you provide to us to receive emails will be stored by us until you log out of our services and will be deleted from both our servers and Sendgrid's servers after you log out.

When processing operational data, ONCARE acts as a data controller responsible for the lawful processing of your personal data.

Types of Data: your name, email address, phone number, date of birth, date of registration, pseudo-keys generated by the App; Device tokens to identify your device, your pseudo-identification number, your IP address, type and version of the operating system used by your device.

When the **myoncare app** is downloaded, the necessary information is transmitted to the app store provider. We have no influence on this data collection and are not responsible for it. We process the personal data provided to us by the provider of the App Store within the framework of our contractual relationship for the purpose of further developing our **myoncare apps** and services.

The app uses the Google Maps API to use geographic information. When using Google Maps, Google also collects, processes and uses data about the use of the map functions. You can find more information about the scope, legal basis and purpose of data processing by Google as well as the storage period in Google's privacy policy.

Purposes of processing operational data: We use the operational data to maintain the functionalities of the **myoncare app** and to contact you directly if necessary or initiated by you (e.g. in the event of changes to the general terms and conditions, necessary support, technical problems, assistance in completing the questionnaires, etc.).

Justification of processing: The processing of company data is justified on the basis of Art. 6 (1) (b) GDPR for the performance of the contract that you conclude with ONCARE for the purpose of using the **myoncare app** .

8. IP GEOLOCATION

We use a geolocation application for our services. We use ipapi (provided by apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Vienna, Austria) and Geoapify (provided by Keptago Ltd., N. Nikolaidi and T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Cyprus) to identify the location of patient users. We use them to secure our applications and verify the location of the patient user to ensure that the use of our services is compliant. We do not combine the information we collect with other information about the user that could identify them. The data processed by apilayer includes the patient's IP address and other location information. The legal basis for the use is Art. 6 para. 1 lit. f GDPR. The data will be deleted when the purpose for which it was collected no longer exists and there is no longer a legal obligation to retain it. For more information about their privacy policies, please visit https://ipapi.com/privacy/

9. PROCESSING OF (TREATMENT) DATA

Applicable to app users who use the app with their service provider.

While using the **myoncare app**, your **service provider** can enter your personal data into the **myoncare portal** in order to start the **myoncare services** (e.g. create you as a patient, provision of an individual task, reminder to take medication, etc.). In addition, you and your **service provider can upload** documents and files to the **myoncare app** and the **myoncare portal** and share them with each other. Your **provider** may upload a **privacy policy** for your information and set other consent requirements for you as a patient for which your consent is required. The files are stored in a cloud database in Germany. Your **service provider** may enable the sharing of such files with other **Portal users** within its institution or other **service providers** outside its facility (consultant physicians) for medical purposes. Other portal users will not have access to these files without this share. In addition, your **service provider** may instruct us to assist you by telephone in filling out questionnaires (outbound calls). This is only done according to the instructions of your service provider and is carried out exclusively by authorized ONCARE employees.

We will use and process your data in accordance with the **terms set out in this Privacy Policy**, provided that you give us your consent where required.

We process this personal data, including your health data, under an agreement with and in accordance with the instructions of your **healthcare provider**. For these processing purposes, the **service provider** is responsible for the processing of your personal data and health data as a data controller within the meaning of the applicable data protection laws, and ONCARE is the data processor of such personal (health) data. This means that ONCARE processes personal data only in accordance with the instructions of the **service provider**. If you have any questions or concerns about the processing of your personal data or health data, you should contact your healthcare provider in the first place .

Types of data: name, date of birth, profile information, contact details and also health data, such as symptoms, photos, information about medications taken, questionnaire responses including disease- or condition-related information, diagnoses and therapies by healthcare professionals, planned and completed tasks.

Purposes of data processing: We process your treatment data in order to provide our **myoncare service** to your **service provider** and to you. Your health data, which you enter into our **myoncare app** , will be used by your **service provider** for advice and support for you. We process this personal data under an agreement with and in accordance with the instructions of your **service provider**. The transmission of this treatment data is pseudonymised and encrypted. To exercise your rights as a data subject, please contact your **service providers**.

Justification of the processing of treatment data: Your personal (treatment) data will be processed by your **service provider** in accordance with the provisions of the **GDPR** and all other applicable data protection regulations. Legal bases for data processing result in particular from Art. 9 (2) (h) GDPR for health data as particularly sensitive data as well as your consent in accordance with Art. 6 (1) (a) and 9 (2) (a) GDPR. The processing of data by ONCARE for its **service providers** is also carried out on the basis of Art. 28 GDPR (Data Processing Agreement).
Your **service provider** is responsible for obtaining your consent as a data controller. Even if you can use the **myoncare app** without such consent, most functions will no longer work (e.g. sharing data with your healthcare provider). The refusal or revocation of consent to the processing of treatment data therefore leads to a severe restriction of the functionality of the app services and your **service providers** can no longer support you via the **myoncare app**.

10. PROCESSING OF ACTIVITY DATA

Only applicable if you agree to and activate activity data transfer via myoncare tools.

myoncare tools offer you the option of connecting the **myoncare app** with certain health apps (e.g. AppleHealth, GoogleFit, Withings) that you use ("**Health App**"). In order to enable the processing of activity data, we obtain your consent to the processing in advance. If the connection is established after your consent, the **activity data collected** by the **Health app** will be made available to your providers to provide additional contextual information about your activity. Please note that activity data is not validated by **myoncare tools** and should not be used by your **healthcare provider** for diagnostic purposes as a basis for medical decision-making. Please also note that your **providers** are not required to verify your activity data and do not have to provide you with feedback on your activity data.
Activity data is shared **with your affiliated** service providers every time the **myoncare app** is accessed . You can revoke your consent to the disclosure of activity data at any time in the settings of the **myoncare app**. Please note that your activity data will no longer be shared from this point on. Activity data that has already been shared will not be deleted from the **myoncare portal** of your affiliated **service providers**.

The processing of activity data is your own data responsibility.

Types of data: The type and amount of data transferred depend on your decision and the availability of that data within the **Health app** . Data may include weight, height, steps taken, calories burned, hours of sleep, heart rate, and blood pressure, among others.

Purpose of Activity Data Processing: Your Activity Data will be provided to your Affiliated **Providers** to provide additional contextual information about your Activity.

Justification of processing: The processing of activity data is your own responsibility.

11. PROCESSING OF PRODUCT SAFETY DATA

Applicable for app users whose service provider uses the medical device variant of the myoncare tools.

The **myoncare app** is classified and marketed as a medical device in accordance with the European Medical Devices Regulations. As the manufacturer of the app, we have to comply with certain legal obligations (e.g. monitoring the functionality of the app, evaluating incident reports that could be related to the use of the app, tracking users, etc.). Additionally, the **myoncare app** allows you and your **healthcare provider** to communicate and collect personal information about specific medical devices or medications used in your treatment. The manufacturers of such medical devices or medicinal products also have legal obligations with regard to market surveillance (e.g. collection and evaluation of side effect reports).

ONCARE is the data controller for the processing of product safety data.

Types of data: Case reports, personal data provided in an incident report, and results of the evaluation.

Processing of product safety data: We store and evaluate all personal data in connection with our legal obligations as a manufacturer of a medical device and transmit this personal data (as far as possible after pseudonymization) to competent authorities, notified bodies or other data controllers with supervisory duties. In addition, we store and transfer personal data related to medical devices and/or medicines when we receive communications from your **healthcare provider**, from you as a patient or from third parties (e.g. our distributors or importers of the **myoncare tools** in your country) that must be reported to the manufacturer of the product in order for it to comply with its legal obligations on product safety.

Justification of the processing of product safety data: The legal basis for the processing of personal data for the fulfilment of legal obligations as a medical device or pharmaceutical manufacturer is Art. 6 (1) (c), Art. 9 (2) (i) GDPR in conjunction with the post-market monitoring obligations under the Medical Devices Act and the Medical Devices Directive (regulated from 26 May 2021 in Chapter VII of the new Medical Devices Regulation (EU) 2017/745) and/or the Medicines Act.

Supplement to the exclusion of liability for side effects:
Oncare GmbH does not undertake any medical evaluation of the transmitted content and is not obliged to forward information relevant to pharmaceutical law such as side effects, application errors or product defects to authorities. This responsibility lies exclusively with the treating service providers or – if affected – with the respective manufacturers of the products used.

12. PROCESSING OF HEALTH AND TREATMENT DATA

Applicable to app users who use the app with their service provider for reimbursement purposes.
The **myoncare app** supports your **healthcare provider** in initiating standard procedures for reimbursement of the healthcare services provided to you via the **myoncare app**. In order to enable the reimbursement process, the **myoncare app** supports the collection of your personal (health) data by your **service provider** for the purpose of transmitting this data to your paying entity (either the Association of Statutory Health Insurance Physicians and/or your health insurance company). This data processing is only an initial data transfer for the **service provider** to obtain reimbursement from your health insurance company. The type and amount of personal data processed does not differ from other reimbursement routines of the **Service Provider**. Your service provider is the Data Controller for Reimbursement Data. ONCARE acts as a data processor on the basis of the data processing agreement with your **service provider**.

Types of data: name, diagnosis, indications, treatment, duration of treatment, other data necessary for the management of reimbursement.

Processing of reimbursement data: Your **provider** transmits the treatment data required for reimbursement to the payer (either its statutory health insurance institution and/or your health insurance company), and the payer processes the reimbursement data in order to provide reimbursement to your **provider** .

Justification of the processing of reimbursement data: The reimbursement data is processed on the basis of §§ 295, 301 SGB V, Art. 9 para. 2 lit. b GDPR. Data processing by ONCARE for your **service provider** is also carried out on the basis of Art. 28 GDPR (order processing agreement).

13. PROCESSING BY DEVICE MANUFACTURERS, MEDICAL DEVICE DISTRIBUTORS AND LABORATORY SERVICE PROVIDERS

If you use additional medical functions such as integrated diagnostics, vital signs collection or laboratory services via the Platform, personal health data may be collected and processed by external third-party providers (e.g. medical device manufacturers, distributors of such or laboratory service providers). This is done to support medical care and always on the basis of explicit consent or a treatment relationship.
The processing is carried out either within the framework of order processing or – depending on the provider – under its own responsibility under data protection law. Oncare GmbH only provides the technical connection for this purpose, without checking or medically evaluating content. Further information on the respective data processing can be obtained directly from the treating service provider or via the data protection information of the integrated third-party providers.

14. COMMERCIAL STORE DATA AND PATHWAY MANAGEMENT

The myoncare portal offers registered service providers (e.g. doctors) the opportunity to offer and configure digital care pathways via a webshop functionality (e.g. in cooperation with myon.clinic) and to assign patients individually.
As part of the use of this functionality, personal data – in particular health data – is processed, such as information on indication, recommended duration of treatment or pathway assignment. This data processing serves the individualization and assignment of medical content and is carried out on the basis of Art. 6 (1) (b) and Art. 9 (2) (h) GDPR.

Oncare provides the technical infrastructure and processes the data concerned as a data controller within the meaning of Art. 4 No. 7 GDPR, insofar as the processing is necessary for the provision of the platform functions. However, the selection of content and medical design of the pathways is the sole responsibility of the respective service provider.
Insofar as billing or data transmission is carried out to third parties (e.g. billing offices or platform partners such as myon.clinic), such processing only takes place on the basis of corresponding agreements or legal regulations.

15. PROCESSING OF OCCUPATIONAL HEALTH MANAGEMENT DATA

Applicable to users of the app who use the app with the company's occupational health management system.

During the use of the **myoncare app** in **the company's occupational health management**, certain personal (health) data is passed on in aggregated form as data for occupational health management to the **company** and the **data providers** commissioned **by the company** (e.g. data analysts or research companies). Neither the **Company** nor any **data service provider** can associate such data with your identity. ONCARE recommends **that you do not share any personal data** while using myoncare services as part of occupational health management.

This means that ONCARE and all **data providers will** only process the data for occupational health management in accordance with the company**'s** instructions . We process such data for occupational health management, including your health data, on the basis of an agreement with your **company** and/or a **data provider** and in accordance with their instructions. For the purposes of this Agreement, the **Company** or the **data provider** is the data controller for the processing of your data for occupational health management purposes, and ONCARE and any **data providers** engaged by the **Company** are the data processors of such data. If you have any questions or concerns about the processing of your data for occupational health management, you should contact the company in the first place **.**

Purposes of data processing in occupational health management: We process your data for occupational health management in order to be able to offer you and the **company** our **myoncare services**. Your occupational health management data, which you enter into our **myoncare app**, will be used by the **company** (either directly or via a **data provider**) as part of occupational health management. We process this data for occupational health management within the framework of an agreement with and in accordance with the instructions of the **company** and/or a **data provider** for its occupational health management. The transmission of this data for occupational health management is pseudonymised and encrypted. To exercise your rights as a data subject, please contact the **Company**.

Justification of the processing of occupational health management data: Your occupational health management data will be processed by the **Company** in accordance with the provisions of the **GDPR** and all other applicable data protection regulations. The legal basis for data processing is, in particular, your consent in accordance with Art. 6 (1) (a) and Art. 9 (2) (a) a GDPR or another legal basis applicable to the **Company**. The processing of data by ONCARE on behalf of the **Company** (either directly or through a service provider commissioned by your Company) is also based on Art. 28 GDPR (Data Processing Agreement).
The **Company** , as a data controller, is responsible for obtaining your consent where required by data protection regulations and processing the data for occupational health management purposes in accordance with applicable data protection laws.

16. WHAT TECHNOLOGY IS USED BY THE MYONCARE APP?

Email service

We use Brevo (provided by Sendinblue GmbH, located at Köpenicker Straße 126, 10179 Berlin) and Sendgrid (provided by Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). These email services can be used to organize the sending of emails. Sendgrid is used to send confirmation emails, transaction confirmations, and emails with important information about requests. The data you enter for the purpose of receiving e-mails will be stored on Sendgrid's servers. When we send emails on your behalf through SendGrid, we use an SSL secured connection.

Email communication is used for the following tasks:

- Logging into the web application for the first time;
- resetting the password for the web application;
- Create an account for the patient application;
- Reset the password for the patient application;
- Preparation and dispatch of a report;
- Replace push notifications with emails for **PWA** (Progressive Web App) in the following cases:
  - → if a care plan ends in an hour;
  - → if medication has been assigned;
  - → if the Privacy Policy has been updated;
  - → when an appointment is sent to patients and doctors, in particular for the "video call" appointment type;
  - → Any information related to a **caretask** or if a **provider** has assigned **a** caretask.

Brevo (Privacy Policy):
Privacy Policy - Personal Data Protection | Brevo

SendGrid (Privacy Policy):
https://sendgrid.com/resource/general-data-protection-regulation-2/

Matomo

This is an open-source web analysis tool. Matomo (provided by InnoCraft Ltd., New Zealand) does not transmit data to servers that are outside of ONCARE's control. Matomo is initially disabled when you use our services. Only if you agree to this, your user behavior will be recorded anonymously. If this is disabled, a "persistent cookie" will be stored, if your browser settings allow it. This cookie signals to Matomo that you do not want your browser to be recorded.
The usage information collected by the cookie is transmitted to our servers and stored there so that we can analyze user behavior.
The information generated by the cookie about your use is:

- Role;
- geolocation of the user;
- User operating system;
- time the user has used content;
- -IP address;
- Websites visited via the web/ **PWA** (for more information, see the section on PWA in this Privacy Policy);
- Buttons that the user **clicks on in the** myoncare portal**, the** myoncare app **and the** myoncare PWA.

The information generated by the cookie will not be shared with third parties.

You can refuse the use of cookies by selecting the appropriate settings in your browser. However, please note that you may not be able to use all the features in this case. For more information, please visit:
https://matomo.org/privacy-policy/ .

The legal basis for the processing of users' personal data is Art. 6 para. 1 sentence 1 lit. a GDPR. The processing of users' personal data enables us to analyse usage behaviour. By evaluating the data obtained, we are able to compile information about the use of the individual components of our services. This helps us to continuously improve our services and their usability.

We process and store personal data only for as long as it is necessary to fulfil the intended purpose.

17. SECURE TRANSFER OF PERSONAL DATA

We use appropriate technical and organisational security measures to optimally protect your personal data stored by us against accidental or intentional manipulation, loss, destruction or access by unauthorised persons. The security levels are continuously reviewed in cooperation with security experts and adapted to new security standards.

Data exchange to and from the app is encrypted. We use TLS and SSL as encryption protocols for secure data transmission. Data exchange is also encrypted throughout and is carried out with pseudo-keys.

18. DATA TRANSFERS / DISCLOSURE TO THIRD PARTIES

We will only pass on your personal data to third parties within the framework of the legal provisions or on the basis of your consent. In all other cases, the information will not be disclosed to third parties, unless we are obliged to do so due to mandatory legal regulations (disclosure to external bodies, including supervisory or law enforcement authorities).

Any transmission of personal data is encrypted in transit.

19. GENERAL INFORMATION ON CONSENT TO DATA PROCESSING

Your consent also constitutes consent to data processing under data protection law. Before you give your consent, we will inform you about the purpose of the data processing and your right to object.

If the consent also relates to the processing of special categories of personal data, the myoncare app will expressly inform you of this as part of the consent procedure.
Processing of special categories of personal data in accordance with Art. 9 (1) GDPR may only take place if this is required by law and there is no reason to believe that your legitimate interests preclude the processing of this personal data or that you have given your consent to the processing of this personal data in accordance with Art. 9 (2) GDPR.
For the data processing for which your consent is required (as explained in this Privacy Policy), consent will be obtained as part of the registration process. After successful registration, the consents can be managed in the account settings of the myoncare app.
A revocation of your consent is only effective for the future. The processing carried out up to the time of revocation remains lawful (Art. 7 para. 3 GDPR).

20. DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

In our organization, we ensure that only those individuals are authorized to process personal data that is necessary to fulfill their contractual and legal obligations. Your personal and health data that you enter into our **myoncare app** will be made available to your **healthcare provider** and/or your **company**, either directly or through a **data provider** (depending on the type of use of the **myoncare tools**).

In certain cases, service providers support our specialist departments in the fulfilment of their tasks. The necessary data protection agreements have been concluded with all service providers who are processors of personal data. These service providers are Google (Google Firebase), cloud storage providers, and support service providers.

Google Firebase is a "NoSQL database" that enables synchronization between the **myoncare portal of your service provider** and the **myoncare app** . NoSQL defines a mechanism for storing data that is not only modeled in tabular relationships by allowing for easier "horizontal" scaling compared to tabular/relational database management systems in a cluster of machines.
For this purpose, a pseudokey of the **myoncare app is stored in Google Firebase** together with the corresponding **medication plan**. The data transfer is pseudonymised for ONCARE and its service providers, which means that ONCARE and its service providers cannot establish a relationship with you as a data subject. This is achieved by encrypting the data in transit between you and your **service provider** or **company** (either directly or to a **data provider**) and using pseudokeys instead of personal identifiers such as name or email address to track these transfers. The re-identification takes place as soon as the personal data has reached the account of your **service provider** or company in the **myoncare portal** or your account in the **myoncare app**, after it has been verified by special tokens.

Our cloud storage providers offer cloud storage, which stores the Firebase manager that manages the Firebase URLs for the **myoncare portal**. In addition, these service providers provide the isolated server domain of the **myoncare portal**, where your personal data is stored. It also hosts myoncare's video and file management services, which enable encrypted video conferencing between you and your **service provider**, as well as file sharing. Access to your personal data by you and your **service provider** is ensured by sending specific tokens. This personal data is encrypted in transit and at rest and pseudonymised for ONCARE and its service providers. ONCARE's service providers do not have access to this personal data at any time.

Furthermore, we use service providers to process service requests (support service providers) regarding the use of the account, e.g. if you have forgotten your password, want to change your saved email address, etc. The necessary order processing agreements have been concluded with

these service providers; In addition, the employees entrusted with processing service requests have been trained accordingly. Upon receipt of your service request, you will be assigned a ticket number.
If this is a service request regarding your account usage, the relevant information you provided to us when contacting us will be forwarded to one of the authorized employees of the external service. He will then contact you.
Otherwise, it will continue to be processed by specially approved ONCARE staff, as described under "PROCESSING OF OPERATIONAL DATA".

Through our support service providers, we use the RepairCode tool, also known as Digital Twin Code, a customer experience platform for handling external feedback with the ability to create support tickets. Here you can find the privacy policy:
https://app.repaircode.de/?main=main-client – Legal/privacy.
Finally, we show you content from Instagram (provider: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland) (e.g. images, videos or posts). When you click on a linked Instagram post, you will be redirected to Instagram. Instagram can set cookies and process user data.

When you visit a page with linked Instagram posts, your browser can automatically connect to Instagram's servers. This gives Instagram the information that you have visited our website, even if you do not have an Instagram account or are not logged in. If you are logged in, Instagram can assign the visit to your user account.

Privacy Policy: https://privacycenter.instagram.com/policy

21. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

To provide our services, we may use service providers who are located outside the European Union. If the data is transferred to a third country where the protection of personal data has not been judged to be adequate, we will ensure that appropriate measures are taken in accordance with national and European law and, if necessary, that appropriate standard contractual clauses have been agreed between the processing parties.
The personal data collected by this **myoncare app** is not stored in the app stores. A transfer of personal data to third countries (outside the European Union or the European Economic Area) only takes place if this is necessary for the fulfilment of the contractual obligation, is required by law or you have given us your consent.

The synchronization of the **myoncare app** and the **myoncare portal** is done via Google Firebase. The Google Firebase server is hosted in the European Union. However, as described in Google Firebase's Terms of Service, short-term data transfers may be made to countries where Google or its service providers are located; For certain Google Firebase services, data is only transferred to the United States, unless the processing takes place in the European Union or the European Economic Area. Unlawful access to your data is prevented with end-to-end encryption and secure access tokens. Our servers are hosted in Germany and for US customers in the USA. For analysis purposes, the emails sent with SendGrid contain a so-called "tracking pixel" that connects to Sendgrid's servers when the email is opened. This can be used to determine whether an e-mail message has been opened.

We embed content from Instagram provided by Meta Platforms Ireland Ltd. If you click on a linked Instagram post, personal data (e.g. IP address, browser information, interactions) may be transmitted to Meta Platforms Inc. in the USA or other third countries.
Meta is certified under the EU-U.S. Data Privacy Framework (DPF), which recognises an adequate level of data protection for transfers to the USA. Nevertheless, data can also be transferred to countries for which there is no adequacy decision by the European Commission. In such cases, additional protective measures may be necessary, but their effectiveness cannot always be guaranteed.

Legal basis
Data processing is based on your consent (Art. 6 para. 1 lit. a GDPR). You can revoke this consent at any time. The lawfulness of the data processing operations that have already taken place remains unaffected by the revocation.

Please note that your data will usually be transmitted by us to a SendGrid server in the USA and stored there. We have concluded a contract with Sendgrid that contains the EU Standard Contractual Clauses. This ensures that there is a level of protection comparable to that of the EU. In addition, additional technical protection measures have been implemented, such as end-to-end encryption and strict access restriction through role-based tokens. This serves to further secure the data transfer in the sense of the "Schrems II" ruling of the ECJ.

To process activity data, interfaces to Google Cloud services (in the case of GoogleFit) or to AppleHealth or Withings are used on the app user's mobile device. **myoncare tools** use these interfaces, provided by Google, Apple, and Withings, to request activity data from connected health apps. The request sent by the **myoncare tools** does not contain any personal data. Personal data is made available to **myoncare tools** via these interfaces.

22. DURATION OF STORAGE OF PERSONAL DATA

We will keep your personal data for as long as it is necessary for the purpose for which it is processed. Please note that numerous retention periods require the continued storage of personal data. This applies in particular, but not exclusively, to retention obligations under commercial or tax law (e.g. Commercial Code, Tax Act, etc.). In addition, your **healthcare provider** must also ensure the retention of your medical records (between 1 and 30 years, depending on the type of documents).

Please note that ONCARE is also subject to retention obligations that are contractually agreed with your **service provider** on the basis of legal provisions. In addition, and only if your **service provider uses** the medical device variant of the **myoncare tools**, certain retention periods resulting from the Medical Devices Act apply due to the classification of the **myoncare app** as a medical device. Unless otherwise retained, the personal data is routinely deleted as soon as the purpose has been achieved.

In addition, we may retain personal data if you have given us your consent to do so or if a dispute arises and we use evidence within the statutory limitation periods, which can be up to 30 years. The regular limitation period is three years.

23. OBLIGATION TO PROVIDE PERSONAL DATA

Various personal data are required for the establishment, implementation and termination of the contractual relationship and the fulfilment of the associated contractual and legal obligations. The same applies to the use of our myoncare app and the various functions it offers.

We have summarized the details for you under the points mentioned above. In certain cases, personal data must also be collected or made available in accordance with the law. Please note that without the provision of this personal data, it is not possible to process your request or fulfil the underlying contractual obligation.

24. ACCESS RIGHTS

For all devices, regardless of the operating system used, it is necessary to grant the app certain permissions, which we call "basic access rights". Depending on the operating system of the device you are using, it may have additional features that require additional permissions for the app to work. In order for the **myoncare app** to work on your device, the app must be granted various permissions to access certain features of the device. If necessary, we will list them in order of the operating system (Android or iOS) according to the "Framework".
The basic access rights (Android and iOS) are:

Get Wi-Fi connections
Required to ensure the functionality of document download in conjunction with Wi-Fi connections.

Get Network Connection
Required to ensure document download functionality in conjunction with network connections that are not Wi-Fi connections.

Deactivate screen lock (prevent stand-by mode)
Required so that the videos that belong to the provided documents can be played directly in the app without being interrupted by a screen lock.

Access to all networks
Access to all networks is required to download documents.

Disabling sleep mode
This is necessary so that the videos that belong to the provided documents can be played directly in the app without the playback being interrupted by the occurrence of hibernation.

Mobile Data / Mobile Data Access
If the user wants to download documents exclusively via Wi-Fi, he can make the appropriate setting in the app's menu and deactivate the use of mobile data. Access to mobile data is required to ensure the functionality of disabling document downloads over mobile data.

Accessing the camera
Camera access is required for both QR code scanning and video consultations

Accessing the microphone
Microphone access is required for video consultations

Access files and photos
This is required for the exchange of files between you and your connected portal users.

Web browser access
This is required to view received files from users of the connected portal.

We use push notifications, which are messages that are sent to your mobile device as a service of the **myoncare app** through services such as the Apple Push Notification Service or the Google Cloud Messaging Service. These services are standard features of mobile devices. The Service Provider's Privacy Policy governs the access, use, and disclosure of personal information as a result of your use of these services.

25. AUTOMATED DECISIONS ON A CASE-BY-CASE BASIS

We do not use purely automated processing to make decisions.

26. YOUR RIGHTS AS A DATA SUBJECT

We would like to inform you about your rights as a data subject. These rights are set out in Articles 15 to 22 of the GDPR and include:

Right of access (Art. 15 GDPR): You have the right to request information about whether and how your personal data is being processed, including information about the purposes of processing, recipients, storage period and your rights to rectification, deletion and objection. You also have the right to receive a copy of any personal data we hold about you.

Right to erasure / right to be forgotten (Art. 17 GDPR): You can request that we delete your personal data collected and processed by us without undue delay. In this case, we will ask you to delete the **myoncare app** including your UID (Unique Identification Number) from your smartphone/mobile phone. Please note, however, that we can only delete your personal data after the expiry of the statutory retention periods.
Right to rectification (Art. 16 GDPR): You can ask us to update or correct inaccurate personal data or to complete incomplete personal data.
Right to data portability (Art. 20 GDPR): In principle, you can request that we provide you with personal data that you have provided to us and that is processed automatically on the basis of your consent or the performance of a contract with you in machine-readable form so that it can be "ported" to a substitute service provider.

Right to restriction of data processing (Art. 18 GDPR): You have the right to request the restriction of the processing of your personal data if the accuracy of the data is contested, the processing is unlawful, the data is needed to assert legal claims or an objection to the processing is being examined.

Right to object to data processing (Art. 21 GDPR): You have the right to object to our use of your personal data and to withdraw your consent at any time where we are processing your personal data on the basis of your consent. We will continue to provide our services even if they are not dependent on withdrawal of consent. A revocation is only effective for the future. The processing carried out up to the time of the revocation remains lawful.

To exercise these rights, please first contact your **service provider** or **company** or contact us at: privacy@myoncare.com . Objection and revocation of consent must be declared in text form to privacy@myoncare.com .

We require you to provide sufficient proof of your identity to ensure that your rights are protected and that your personal data will only be shared with you and not with third parties.

Please also contact us at any time at privacy@myoncare.com if you have any questions about data processing in our company or if you would like to withdraw your consent. You also have the right to contact the competent data protection supervisory authority.

27. DATA PROTECTION OFFICER

You can reach our data protection officer for all questions about data protection at privacy@myoncare.com.

28. AGE RESTRICTION OF APPLICATION

A minimum age of 18 years is required to use the **myoncare app** .

29. CHANGES TO THE PRIVACY POLICY

We expressly reserve the right to change this **Privacy Policy** in the future at our sole discretion. Changes or additions may be necessary, for example, to comply with legal requirements, to take account of technical and economic developments or **to do justice to** the interests of app **or** portal users. Changes are possible at any time and will be communicated to you in an appropriate manner and in a reasonable timeframe before they become effective (e.g. by posting a revised Privacy Policy at login or by giving advance notice of material changes).

In the event of questions of interpretation or disputes, only the German version of the privacy policy is binding and authoritative.

ONCARE GmbH Postal address: Balanstraße 71a, 81541 Munich, Germany

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

Contact details of the Data Protection Officer: privacy@myoncare.com

For transactions in the myoncare store – especially in connection with treatment plans (pathways) – the economic and content-related responsibility lies with myon.clinic GmbH, a subsidiary of Oncare GmbH. In this context, Oncare GmbH only provides the technical platform.

Last updated in June 2025.

* * *

The following are the supplementary data protection regulations for users in the United States of America:

HIPAA protects personally identifiable health information (PHI) only if it is processed in the context of the U.S. healthcare system by a HIPAA-compliant entity – i.e., a covered entity or business associate – regardless of the data subject's citizenship or residency.

US Supplementary Privacy Policy for Users in the United States of America (HIPAA)

Scope:
This section supplements the Privacy Policy for users residing in the United States of America (USA) or for cases where Protected Health Information (PHI) is processed pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

It applies in all states of the USA insofar as ONCARE or commissioned partners process health data as a *business associate* on behalf of *covered entities* (e.g. doctors or clinics) in the context of treatment processes.

1. Legal basis in the USA

The processing of personal health information in the U.S. is governed by the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and subsequent amendments, including, but not limited to:

- HIPAA **Privacy Rule** (45 CFR Part 160 & Subparts A and E of Part 164)
- HIPAA **Security Rule** (Subparts A and C of Part 164)
- **HIPAA Breach Notification Rule** (Subpart D of Part 164)
- and, in addition, the HITECH Act of 2009

These regulations apply regardless of which state of the USA the patient or the processing agency is in.

2. ONCARE's role as a business associate

ONCARE GmbH and affiliated companies in the USA act exclusively as so-called **business associates** within the meaning of HIPAA when they **provide services in connection with the processing of PHI on behalf of healthcare providers *(*covered entities**). A Business Associate Agreement (BAA) pursuant to 45 CFR §164.504(e) governs the data protection obligations to these entities. In this context, ONCARE undertakes:

- Provision of the myoncare platform (video, communication, monitoring)
- Technical Data Processing & Hosting
- Provision of algorithmic support functions (e.g. triage)

ONCARE does not provide **medical services** and **does not make medical decisions** in the sense of diagnosis, therapy or prescription.

3. Type of data processed (PHI)

For the purposes of HIPAA, PHI is defined as any information that:

- relate to the health status or treatment of an identifiable patient, and
- in connection with a *Covered Entity* or its Business Associate.

The PHI processed by ONCARE include, in particular:

- Medical history (symptoms, risk factors)
- Monitoring data (vital signs, wearable data)
- User interactions within structured questionnaires or triage tools
- Communication Histories with Healthcare Providers

4. Patients' Rights under HIPAA

Every affected user in the U.S. has the right to:

- **Information** about the PHI stored about him (45 CFR §164.524)
- **Correction** of Incorrect or Incomplete PHI (45 CFR §164.526)
- **Limitation** of Disclosure or Use in Certain Cases (45 CFR §164.522)
- **Confidential communication** at the request of the patient
- **Objecting** to certain disclosures (to the extent permitted by law)
- **Accounting** of Disclosures (45 CFR §164.528)
- **Complaint** to the U.S. Department of Health and Human Services (Office for Civil Rights)

ONCARE provides technical interfaces to implement these rights on request.

To assert these rights, you can make an informal request via the myoncare app or contact us by e-mail. Implementation usually takes place within 30 days in accordance with 45 CFR §164.524 et seq. If the request is complex, the deadline can be extended once by a further 30 days. ONCARE provides digital export formats and access interfaces for this purpose.

5. Security Measures in Accordance with Security Rule

ONCARE is committed to complying with all requirements of the HIPAA Security Rule, including:

Administrative measures

- Internal data protection and access concepts
- Written guidelines on access regulation
- Risk analyses and regular audits
- Employee training with a HIPAA focus

In addition, ONCARE is committed to regularly conducting a structured "Security Risk Assessment" in accordance with 45 CFR §164.308(a)(1)(ii)(A) to identify, assess and take appropriate action on security risks.

Technical measures

- Encryption of all PHI at rest and in transit
- Role-based access control
- Logging and access history
- Two-Factor Authentication for Medical Staff

Physical measures

- Secure server locations with access control
- Disaster Recovery Concepts
- Hardware and endpoint access restrictions

6. Data protection in automated triage

The myoncare platform contains a structured triage function that evaluates patient information (e.g. symptoms) based on defined criteria and creates **a technical risk assessment**.

This feature:

- **does not replace a medical diagnosis**,
- **does not independently decide on treatment or intervention**,
- **only informs authorized service providers** (covered entities) of potentially relevant information.

ONCARE bears no medical responsibility for decisions made by doctors or clinics on the basis of this information.

7. Disclosure of PHI and other uses

ONCARE only shares PHI with:

- to eligible healthcare providers in the context of care,
- to supervisory authorities if required by law,
- for security incidents under the **Breach Notification Rule** (within 60 days of knowledge pursuant to 45 CFR §164.404),
- never for advertising, distribution, or third-party use purposes without the patient's express, documented consent.

Any disclosure or use of PHI for research, marketing or other third-party purposes will only take place after prior documented authorization in accordance with 45 CFR §164.508. Without this express consent, no such disclosure will take place.

Use of De-identified Data for Commercial Purposes
ONCARE may use health and usage data that have been de-identified in accordance with the HIPAA Privacy Rule (45 CFR §164.514) for internal analysis, platform improvement, development of new healthcare services, and other commercial purposes.

Once data are de-identified, they are no longer considered Protected Health Information (PHI) and are not subject to the protections of the HIPAA Privacy Rule.

8. Contact for the exercise of rights

Responsible for HIPAA-related concerns:
ONCARE GmbH
Balanstraße 71a80339 MunichGermanyE-mail: privacy@myoncare.com

U.S. citizens can also contact the **U.S. Department of Health and Human Services – Office for Civil Rights (OCR)** directly with complaints: https://www.hhs.gov/ocr/

9. Integration of third-party providers, webshop data and disclaimer

9.1 Involvement of technical third-party providers (device manufacturers, medical device distributors and laboratories)

Within the framework of the myoncare platform and its subsidiary myon.clinic, **third-party providers such as device manufacturers, distributors of medical devices or medical laboratories** can be connected to the system if required. This is done exclusively to support medically responsible care and is based on the instructions of the respective *covered entities*.

The connected third-party service providers process personally identifiable health information (PHI) only under contractual agreement and in compliance with HIPAA requirements. You are also subject to the data protection requirements of 45 CFR §164.502(e) as a *subcontractor* of a business associate and are bound by corresponding **subcontracting agreements (sub-BAA**).

9.2 Data collection in the context of webshop offers

When purchasing digital health programs, so-called digital health programs. **Pathways**, or affiliate products via the webshop of the subsidiary **myon.clinic**, personal data, including PHI, may be processed for the purpose of processing and maintaining these programs. This applies in particular:

- Usage data of the Pathway functionality,
- specified symptom or diagnostic data,
- any redeemed health codes or product information.

The collection is carried out in compliance with the HIPAA Privacy and Security Rules and exclusively for a specific purpose. Disclosure to third-party providers will only take place on the basis of an existing sub-BAA or with documented consent.

Any disclosure of PHI (Protected Health Information) outside the contract chain (e.g. for research or marketing) requires a documented **"authorization"** according to 45 CFR §164.508.

9.3 Disclaimer for Medical Evaluation and Side Effects

ONCARE GmbH and its affiliated companies do not assume **any medical evaluation or obligation to report adverse drug reactions, product side effects or other health-related risks.**

Legal responsibility for:

- the diagnosis and selection of a pathway or product,
- the assessment of risks or contraindications,
- as well as the legally required **reporting of side effects** or safety events to regulatory authorities or manufacturers

lies exclusively with the attending physician or the offering **covered entity** or the responsible device or drug manufacturer.

The platform **only provides the technical infrastructure** and does not assume any medical or regulatory responsibility for the content, results or consequences of any application by patients or service providers.

Preemption Rule & State Law Compliance

The Health Insurance Portability and Accountability Act (HIPAA) provides a **minimum level of data protection under federal law** that applies in all U.S. states. At the same time, 45 CFR §160.203 allows for so-called **preemption**, i.e. stricter regulations by individual states can override HIPAA in certain respects if they:

- ensure greater protection for data subjects, or
- special requirements for health data or electronic health data.
- ONCARE and its affiliates are expressly committed to complying with all relevant federal laws, including, but not limited to:

- **California Consumer Privacy Act (CCPA/CPRA)**
- **Texas Medical Privacy Act (TMPA)**
- **New York SHIELD Act**
- **Massachusetts Data Security Regulations**
- as well as comparable data protection laws at the state level

To the extent that ONCARE acts on behalf of Covered Entities, the processing is carried out in compliance with both HIPAA and applicable state data protection standards, provided that these are stricter than HIPAA requirements. In the event of deviations, the regulation that **offers the patient concerned a higher level of data protection** always applies.

In addition to the nationwide HIPAA regulations, additional data protection laws apply in individual states – such as California, New York or Texas. To the extent that these laws have stricter requirements than HIPAA, they take precedence. In these cases, ONCARE will comply with the strictest applicable law.

11. Exercising HIPAA Rights (Procedures, Identity Verification, Time Limits)

Users residing in the U.S. or whose data is processed by U.S. covered entities have the rights set forth in Section 4 of this Privacy Policy in accordance with HIPAA.

The following regulations apply to the exercise of these rights:

11.1 Application

HIPAA rights may be exercised by:

- written request by e-mail to: **privacy@myoncare.com**
- Written request about the respective healthcare provider (*covered entity*)

11.2 Identity Verification

For the protection of the data subject, any request for the exercise of rights will only be processed after **successful verification of the identity**. Possible measures include:

- Comparison with data used during registration
- Presentation of a valid photo ID (in secure upload)
- Confirmation from the attending physician

11.3 Processing Deadlines

ONCARE processes requests:

- **within 30 calendar days** from the date of receipt of the application,
- Extension for **a further 30 days** is permissible once; the applicant is informed in writing and receives the justification
- all inquiries and responses will be documented and archived in accordance with 45 CFR §164.530(j).

12. Data Processing Outside the United States (Offshoring / Data Localization)

In certain cases, the processing of PHI may be carried out on behalf of a U.S. covered entity **outside the United States**, in particular:

- by ONCARE GmbH, established in Germany (EU),
- to provide technical infrastructure services, hosting, support and product development.

This cross-border processing is carried out exclusively:

- on the basis of an existing **Business Associate Agreement** (BAA),
- with explicit documentation in the HIPAA Risk Management Plan of the Covered Entity,
- with compliance with the HIPAA Security Rule as well as supplementary **security measures according to the European GDPR standard**, in particular:
  - → End-to-end encryption (AES-256),
  - → Access restriction according to the need-to-know principle,
  - → Logging of all accesses with audit trail,
  - → Data storage only on servers with physical access control and ISO 27001 certification.

PHI is **not stored on systems outside the USA without appropriate technical protection measures** and contractual protection.

Administrative Safeguards

ONCARE has implemented administrative measures under 45 CFR §164.308 for all U.S.-related services, including:

- **Data Protection Officers and HIPAA Enterprise-Level Officers**
- **Privacy and security policies**, versioned, documented, and backed by training
- **Mandatory training for all employees** who work with US health data (at least annually)
- **Sanctions Rules** for Data Protection Violations as defined by 45 CFR §164.530(e)
- **Risk-based system assessment and vulnerability assessments**, at least annually or in the event of significant system changes

All processes are documented in an internal **HIPAA compliance manual**, which is regularly updated and reviewed in the internal audit.

14. HIPAA Security Rule Technical Safeguards

ONCARE has fully implemented technical protection measures in accordance with 45 CFR §164.312:

Category	Measure
Access Control	Role-based access, unique user IDs, automatic session logout, emergency access procedures
Audit Controls	Complete system and access logging with regular evaluation
Integrity Controls	Hash-based integrity checks and version control for critical medical data
Authentication	Two-factor authentication for medical staff and administrators
Transmission Security	TLS 1.3 encryption during transmission, VPN protection for all external service providers

These measures apply to all systems that store, process, or transmit PHI. Implementation is ensured annually by technical penetration tests and a **HIPAA-compliant risk analysis** .

***