# MYONCARE PLATFORM – PRIVACY POLICY SERVICE PROVIDER
## AS OF JUNE 2025

Welcome to myoncare, the digital health portal for efficient and needs-based patient care.
For us at Oncare GmbH (hereinafter referred to as "**ONCARE"** or "**we**", "**we**", "**our**"), the protection of your privacy and all personal data relating to you while using the myoncare portal is of great importance and importance. We are aware of the responsibility that arises from the provision and storage of your personal data in the myoncare portal (= platform). 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.

This Privacy Policy consists of two parts:

• The first part contains data protection regulations for the use of the myoncare platform within Europe on the basis of the General Data Protection Regulation (GDPR).
• The second part contains supplementary provisions in accordance with the requirements of the US Data Protection Act (HIPAA). These apply in particular **if health data is processed by a US covered entity or if service providers operate within the framework of the US healthcare system** – regardless of the residence of the person concerned.

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 find out why and how **ONCARE** processes your personal data that we collect from you or that you provide to us when you decide to use the myoncare portal. In particular, you will find a description of the type of personal data we collect and process, as well as the purpose and basis on which we process the personal data; in addition, you will find the rights to which you are entitled here.

Please read the Privacy Policy carefully to ensure that you understand each provision. After reading the Privacy Policy, you will have the opportunity to consent to the Privacy Policy and consent to the processing of your personal data as described in the Privacy Policy. If you give your consent, the Privacy Policy becomes part of the contract between you and ONCARE.

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

### 1. DEFINITIONS

"**App User**" means any user of the myoncare App (your patient).
**"Blockchain technology"** The myoncare system contains an additional database in which the data of all installations is stored.
**"Careplan Provider**" means you or any other service provider or third party (e.g., medical device manufacturer, pharmaceutical company) that makes Care Plans available to other users of the Portal through the myonclinic Store or other means of data exchange.
**"Careplan User**" means you or another service provider (Portal User) who uses a Care Plan ("Pathway") for the treatment of its Registered Patients.
**"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 carried out by the care providers involved, the nursing staff or the patient himself.
"**Provider**" means you or any other physician, clinic, healthcare facility, or other healthcare professional acting alone or on behalf of you or another physician, clinic, or healthcare facility (Intended User).
"**myoncare App**" means the myoncare mobile application for patients who wish to use the services offered by ONCARE through the App.
"**myonclinic Store**" is the platform operated by **ONCARE** that provides digital care concepts (treatment plans) for the treatment of your registered patients via the myoncare portal.
"**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 via the PWA and not via the myoncare App.
"**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 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 you or another service provider using the web-based myoncare Portal.
"**Patient Privacy Policy**" means the Privacy Policy that describes the collection, use and storage of the personal (health) information of Patients using the myoncare App. 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.
"**Privacy Policy**" means this statement provided to you as a user of the myoncare Portal, which describes how we collect, use and store your personal data and informs you of your broad rights.
"**Terms** of Use" means the terms and conditions of use for the use of the myoncare Portal.

### 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 and operates the interactive web portal myoncare Portal (for healthcare professionals) and the mobile application myoncare App (for patients) 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 portal** . For the use of the **myoncare app** by patients, you can find a separate privacy policy for patients here: https://www.myoncare.com/privacy-policy

### 3. WHAT IS PERSONAL DATA

"**Personal Data**" means any information that allows a natural person to be identified. This includes, but is not limited to, your name, birthday, address, phone 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, "**pseudonymised**" 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. (within the meaning of Art. 4 No. 5 GDPR).

**Myoncare PWA**
A Progressive Web App (PWA) is a website that looks and has the functionality of a mobile app. PWAs are designed 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.

## 4. 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 on our **myoncare portal**, contacting us about problems with the portal or otherwise interacting with us for the purpose of using the portal.

**Treatment data**: You collect personal data of your patients, such as name, age, height, weight, indication, symptoms of illness and other information in connection with the treatment of your patients (e.g. in a care plan) in the **myoncare portal**. Activity data of your connected patients is made available to you in your **myoncare portal** .

**Commercial Store Data:** Commercial Store Data: Personal data processed in connection with the use of the myonclinic 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 processed by us when an **app user connects** the **myoncare app** to a health application (e.g. AppleHealth, GoogleFit, Withings). The activity data of your connected patients is made available to you in your **myoncare portal**.

**Analysis of anonymised usage data for platform improvement:**
We only process anonymised, non-personal technical usage data (e.g. aggregated information on usage frequency or system performance) to further develop the functionality and user experience of the portal. These data contain no identifying information and do not allow any conclusions to be drawn about individual portal users. Personal data of healthcare providers is not processed for research or commercial purposes.

**Data from device manufacturers or laboratories:**
In addition, personal data may be processed by connected medical device manufacturers 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 in the event that you report an incident in order to ensure legal certainty or vigilance of medical device or pharmaceutical companies.

**Reimbursement Data:** Personal data required for the reimbursement process.

## 5. BLOCKCHAIN TECHNOLOGY

Blockchain **technology** ("**Blockchain**") (European Patent No. 4 002 787) is an **optional** service that is not mandatory. It is up to you, the **service provider**, to decide 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.
The **blockchain** generally 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. In this case, the block can no longer be synchronized with the others. 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. If all nodes (network nodes) try to synchronize their copies, it is determined that the modified copy has been modified, and the network considers that node to be unhealthy. This technical process prevents unauthorized persons from manipulating the contents of the blockchain chain.

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 authorization to become a user. This structure makes it possible to leverage the security and immutability of **blockchain technology** while remaining data protection compliant, 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 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:**

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

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

When verifying consent to data protection, in case the **provider** wants to communicate with the patient, the system checks whether the patient has agreed to the **provider**'s privacy policy . The **blockchain** thus serves to ensure the integrity and accountability of the protocol 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 agrees to the privacy policy, that interaction is stored on the **blockchain**. Every time there is a communication with the patient, the blockchain responds by comparing the hash to a marker indicating 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 out of sync or does not match the profile on the mobile phone by comparing the hash of the patient profile on 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.

**Justification of processing:** The processing of data by ONCARE on behalf of the **service provider** is carried out on the basis of Art. 28 GDPR (data processing agreement).

**6. OPERATIONAL DATA PROCESSING**

In case you are a contact person for the operation of the Portal at your location/practice (e.g. IT administrator, appointed medical professional), you may provide us with certain personal data when you contact us to understand or discuss the functions and use of the Portal, or in the event of a service request.

In the event of a service request, the following personal data can also be viewed by authorized ONCARE employees:
Your personal data that you have provided to us for registration and/or login to our portal (e.g. name, date of birth, profile picture, contact details).
Authorized ONCARE employees who are authorized to access your database for the purpose of processing a service request are contractually obligated to keep all personal data strictly confidential.

**Important Explanations of 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 Web App) and the **myoncare app** to inform you about tasks, deadlines 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 will ensure that you don't miss any important notifications and that your support runs smoothly.

**Why we do this:**
Our goal is to ensure that you are always informed about your tasks and important updates in order to optimally support your care.
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.

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

**Types of data:** email address, date of birth, date of registration, your IP address, pseudo-keys generated by the portal.

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 portal** and to contact you if necessary or directly initiated by you (e.g. in the event of changes to the terms and conditions, necessary support, technical problems, etc.). In addition, personal data (e-mail address) is processed within the framework of two-factor authentication every time you log in to the **myoncare portal** .

**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 portal** .

## 7. 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 on their privacy policies, please see https://ipapi.com/privacy/ and Privacy Policy |Geoapify location platform.

## 8. PROCESSING OF (TREATMENT) DATA

While using the **myoncare portal**, you enter personal (health-related) data of your patients into the **myoncare portal** (e.g. provision of an individual treatment plan, reminder to take medication, etc.). In addition, you and your patients can upload documents and files to the **myoncare portal** and share them with each other. Furthermore, location functions can be generated and implemented:

- Adding a location;
- Uploading the logo of the website;
- Adding the details of the location;
- Upload a privacy policy;

It is possible to create further consent requirements for the patient, for which the patient must provide consent in order to connect to the website.
An uploaded privacy policy will be displayed to every patient who connects to the website. All declarations of consent must be documented in the uploaded privacy policy. Once a privacy policy has been uploaded, it can only be replaced by a new version, but cannot be deleted.
The files are stored in a cloud database in Germany. You can allow the sharing of such files with other **Portal users** within your institution for medical purposes. Other **portal users** do not have access to these files.
You can also consult a service provider outside your institution (consultant doctor) in the context of the treatment of your patients, if you are of the opinion that another expert opinion serves the treatment.

**In accordance with the GDPR, as a data controller, you are responsible for the processing of patients' health data in the context of the use of myoncare services.**

We process this personal data, including the patient's health data, under an agreement with you and in accordance with your instructions. Please only process your patients' data if you have obtained the necessary data consent from these patients. ONCARE acts as a processor in accordance with the separate data processing agreement we have entered into with you on the basis of Art. 28 GDPR.

## 9. PROCESSING OF TECHNICAL USAGE AND SYSTEM DATA

**Only applies if you use the myonclinic Store as a Careplan user.**
The **myonclinic store** is integrated into the **myoncare portal** and offers the purchase of treatment plans (Careplan). After registering in the **myoncare portal**, you can connect to the **myonclinic store** with your login data . You can use the **myonclinic store** to purchase treatment plans as a user.
**Data of the Careplan user:**

The data of the **Careplan User**, which the **myonclinic Store** processes during use, is processed for the purpose of concluding a license agreement with the **Careplan Provider** – in this case ONCARE – and, if a fee is due, for the processing and control of the payment process between the **Careplan Provider** – in this case ONCARE – and the **Careplan User** .

**Types of data**: name, contact details, bank details.

**Processing of commercial store data:** Personal data processed by us when using the **myonclinic store** as part of the purchase of treatment plans. In addition, the payment data (if a usage fee is charged) will be **forwarded to the Careplan provider** .

**Justification of the processing of commercial store data:** The legal basis for the processing of commercial store data is Art. 6 (1) (b) GDPR – the processing of the data serves the performance of the contract between **the Careplan user** and **the Careplan provider** – in this case ONCARE.

## 10. PROCESSING OF ACTIVITY DATA

**Only applicable if your connected app users consent to and enable data transfer.**

The **myoncare tools** offer **app users** the option of connecting the **myoncare app** to certain health apps (e.g. AppleHealth, GoogleFit, Withings) ("**Health App**"), provided that these are used by the **App User** and the connection is established by the **App User**. Once connected, the activity data collected by the **Health App** will be made available to you to provide additional contextual information regarding the **App User**'s activity . Please note that the activity data **does not originate** from myoncare tools and should therefore not be used for diagnostic purposes as a basis for medical decisions.

The processing of activity data is the responsibility of your patients.

**Types of data:** The type and scope of data transferred depend on the decision of the **app users** . Data includes weight, height, steps taken, calories burned, hours of sleep, heart rate, and blood pressure, among others.

**Purpose of Processing Activity Data: The** App User'**s Activity Data** is provided to you in order to provide additional contextual information regarding the **App User's** activity . Please note that activity data is not validated by **the myoncare tools** and should not be used for diagnostic purposes or as a basis for medical decisions.

**Reason for processing:**
The data controller is the patient himself, by giving you access to his activity data in order to verify the information shared. There is therefore no need for further justification.

## 11. PROCESSING OF PRODUCT SAFETY DATA

**Only applies if you use the medical device variant of the myoncare tools.**

The **myoncare portal** and the **myoncare app** are classified and marketed as medical devices in accordance with the European medical device regulations. As the manufacturer of **the myoncare tools**, we have to comply with certain legal obligations (e.g. monitoring the functionality of the tool, evaluating incident reports that may be related to the use of the tool, tracking users, etc.). In addition, **the myoncare tools** allow you to collect personal data about specific medical devices or medications used in the treatment of your patients. 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 assessment, details of the reporter.

**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 (to the extent possible after pseudonymization) to competent authorities, notified bodies or other data controllers with supervisory obligations. In addition, we store and transfer personal data related to medical devices and/or medicines when we receive communications from you as the reporter of such information, from your 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.

**Rationale for processing product safety data:**
The legal basis for the processing of personal data for the fulfilment of legal obligations as a manufacturer of medical devices or medicinal products 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 BY EQUIPMENT MANUFACTURERS 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 parties (e.g. medical device manufacturers 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.

## 13. 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.

## 12. PROCESSING OF REIMBURSEMENT DATA IN THE EVENT OF COST OBJECT TRANSMISSION

**(Only applicable if you use myoncare tools for reimbursement.)**
The **myoncare portal** supports you in initiating your standard procedures for reimbursement of the healthcare services that you have provided to your patients via the **myoncare app**. To enable the reimbursement process, the **myoncare portal** supports the collection of your patients' personal (health-related) data from the **myoncare portal** in order to facilitate the transmission of this data to the patient's payers as part of the standard reimbursement processes (either your Association of Statutory Health Insurance Physicians and/or the patient's health insurance company). You are the data controller for the reimbursement data and are responsible for complying with data protection regulations for the processing of your patients' personal data in the reimbursement process. ONCARE acts as a Data Processor on the basis of the Data Processing Agreement with the **Service Provider**.

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

**Processing of reimbursement data**: You, as the controller, transmit the patient's treatment data required for reimbursement to the payer (either your health insurance company and/or the patient's health insurance company) and the payer processes the reimbursement data in order to reimburse you.

**Reason for the processing of reimbursement data:** The processing of reimbursement data is carried out on the basis of §§ 295, 301 SGB V. The processing of data by ONCARE for you is also carried out on the basis of Art. 28 GDPR (order processing agreement).

## 13. WHAT TECHNOLOGY IS USED BY THE MYONCARE PORTAL AND THE MYONCARE APP?

The **myoncare portal** works as a web-based tool for which you need a working internet connection and an up-to-date version of the internet browser Chrome, Firefox or Safari.
**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 within one day;
  - → 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.

**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.

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

**SendGrid**
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:

- User's operating system;
- Geolocation of the user;
-Browser;
-Role;
-IP address;
- Websites visited via the Web/PWA (see the section on PWA in this Privacy Policy for more information);
- Buttons that the user clicks in the **myoncare portal**, in the **myoncare app** and in 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 user 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.

## 14. 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 from and to the portal as well as from and to the app is encrypted. We offer SSL as an encryption protocol for secure data transmission. Data exchange is also encrypted throughout and is carried out with pseudo-keys.

## 15. DATA TRANSFERS / DISCLOSURE TO THIRD PARTIES

Your personal data will only be passed on to third parties within the framework of the statutory 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.

The information on how we handle the personal (health) data of your patients who use the **myoncare app** is summarized in a separate **privacy policy** for the **myoncare patient app**. You can find the **privacy policy for patients** here. Please also read this patient privacy policy carefully. You are the data controller for part of the processing of patient data and are responsible for compliance with data protection (e.g. transmission of treatment data to the patient).

## 16. 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 portal** will expressly inform you of this as part of the consent procedure.
Processing of special categories of personal data pursuant to Art. 9 (1) GDPR may only take place if this is necessary due to legal provisions and there is no reason to assume 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 portal** . In addition, ONCARE will ask you to agree to a data processing agreement for the data processed by ONCARE under your responsibility as a controller.

## 17. DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

In our organisation, we ensure that only those persons who are obliged to do so in order to fulfil their contractual and legal obligations are entitled to process personal data.

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 your service provider's myoncare portal 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 portal** and the **myoncare app** is stored in Google Firebase together with the corresponding treatment 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 and using pseudo-keys instead of personal identifiers such as names or email addresses to track these transfers. The re-identification takes place as soon as the personal data has reached the patient account in the **myoncare app** or your account in the **myoncare portal** after verification by specific 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 both your personal data and that of your patients are stored. It also hosts myoncare's video and file management service, which enables encrypted video conferencing and data sharing between you and your patient. Access to your personal data by you and your patient is ensured by sending specific tokens. This personal data is encrypted during

transmission and pseudonymised for ONCARE and its service providers during transmission and at rest. 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 the processing of 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 tool RepairCode, also known as Digital Twin Code. This is a customer experience platform for handling external feedback with the ability to create support tickets. Here you will 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 a linked Instagram post, 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

**18. 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.

Personal data collected by the **myoncare portal** or the **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 portal** with the **myoncare app** is done with the help of Google Firebase. Google Firebase's servers are hosted in the European Union. Nevertheless, according to Google Firebase's general terms and conditions, a temporary transfer of data to countries in which Google and related service providers maintain branches. 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. Unauthorized access to your data is prevented by end-to-end encryption and secure access tokens. Our online servers are hosted in Germany. 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.

**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.

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.

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. The **myoncare tools** use these interfaces, which are provided by Google, Apple and Withings, to request activity data from the 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.

**19. 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 to retention obligations under commercial or tax law.

Please note that ONCARE is also subject to retention obligations that are contractually agreed with you on the basis of legal provisions. In addition, due to the classification and, if applicable, your use of the **myoncare portal** and the **myoncare app** as a medical device, certain retention periods apply to the portal, which result from the Medical Devices Act. 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.

**20. YOUR RIGHTS AS A DATA SUBJECT**

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 portal** and the various functions it offers.

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.

**21. AUTOMATED DECISIONS IN INDIVIDUAL CASES**

We do not use purely automated processing to make decisions.

**22. 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, as well as your rights to rectification, erasure 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 portal** from your computer. 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 concerning you 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.
To exercise these rights, please contact us at: privacy@myoncare.com. Objection and revocation of consent must be submitted to privacy@myoncare.com in text form .
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.

**23. DATA PROTECTION OFFICER**

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

**24. SUBJECT TO CHANGES TO THIS 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 notified to you in an appropriate manner and within a reasonable timeframe prior to their effective date (e.g., by posting a revised **Privacy Policy** upon login or by providing advance notice of material changes).

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

If medical content or services are obtained or offered via the integrated myonclinic store, the content and economic responsibility is borne by myon.clinic GmbH, a subsidiary of Oncare GmbH. In this context, Oncare GmbH only provides the technical platform. privacy@myon.clinic

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

AS OF JUNE 2025

* * *

The following **are supplementary data protection regulations for service providers** who act as a covered entity **in** the United States of America **as part of** a HIPAA-compliant activity **or on behalf of such an entity**:

The protection of personal health information (PHI) under HIPAA only applies if this data is processed within the framework of the U.S. health care system by a so-called covered entity or a business associate – regardless of the nationality or residence of the data subject. The only decisive factor is that the processing falls within the scope of HIPAA.

# US Supplemental Data Protection Regulations for Service Providers in the United States of America (HIPAA)

**1. Scope of Application**

This HIPAA Addendum applies to all service providers who process, store, or share protected health information (PHI) through the ONCARE platform, provided that such processing is in connection with a HIPAA-regulated contractor ("Covered Entity") or ONCARE acts as a business associate.

**2. Roles and responsibilities**

ONCARE is acting as a business associate under the HIPAA Privacy Rule (45 CFR §160.103) and is committed to complying with all applicable HIPAA regulations to the Covered Entity. The respective service provider acts either:

- as a workforce member of the covered entity or
- as a subcontractor of ONCARE in accordance with 45 CFR §160.103 et seq.

**3. Processing frame**

The use of the ONCARE platform by service providers is only based on existing HIPAA-compliant agreements with the covered entity (e.g. business associate agreements or service provider agreements). The processing includes in particular:
- Documentation of treatment courses and medical services,
- Communicating with patients using HIPAA-compliant communication channels (end-to-end encryption, TLS)
- Access to structured patient data for care or quality assurance.

**4. Confidentiality and access control**

Providers agree to keep all PHI confidential and to limit access to PHI to the extent necessary in accordance with the Minimum Necessary Standard (45 CFR §164.502(b)). Every access is managed via a role-based rights concept and logged in an auditable manner.

**5. Technical and organizational security measures**

All security measures implemented by ONCARE comply with the requirements of the HIPAA Security Rule (45 CFR Part 164, Subpart C). These include:

- AES-256 encryption of stored data,
- encrypted transmission via TLS 1.3,
- Two-factor authentication (2FA),
- periodic risk analyses pursuant to §164.308(a)(1)(ii)(A),
- structured incident response processes.

**6. Data processing outside the USA**

When Providers access data through ONCARE that is processed or stored outside the United States (e.g., hosting in the EU), they do so exclusively:
- on the basis of HIPAA-compliant contractual protection (e.g. subcontractor BAA),
- with documented consent from the Covered Entity,
- in compliance with the HIPAA Security Rule and complementary international standards (e.g. B. ISO 27001, GDPR principles),
- and with end-to-end encryption and access control.

**7. Reporting obligations in the event of data protection incidents**

Providers are required to immediately notify ONCARE of any incident that could lead to unauthorized access to PHI ("Security Incident" or "Breach" as defined in 45 CFR §164.304/§164.402). ONCARE takes over the coordination of the legally required reports to the covered entity and affected persons.

**8. Rights of the Covered Entity**

The Covered Entity retains the right at any time to audit the access, use and security measures regarding PHI by ONCARE and Associated Service Providers. Service providers must assure full cooperation.

**9. No independent distribution**

The Service Provider may only disclose PHI to third parties outside the Platform (e.g., by email, external system, printout) if:

- there is a documented "authorization" by the data subject or
- this is expressly provided for in the contract.

**10. Precedence and interpretation**

In the event of any conflict between this HIPAA Supplement and European data protection rules, the stricter rule will always apply, provided that it is consistent with applicable law. U.S. federal privacy laws (e.g., CCPA) remain and state privacy laws, unaffected and apply in addition where applicable.

**11. Support for the rights of data subjects**

Service providers support ONCARE and the respective Covered Entity in fulfilling the rights of data subjects pursuant to 45 CFR §§ 164.524–528 (e.g. information, correction, restriction of disclosure). This includes, in particular, participation in:
- the provision of access logs ("Accounting of Disclosures"),
- the correction of erroneous PHI,
- the implementation of blocking notices or restrictions on use.

Requests will be coordinated by ONCARE and processed with a notice period of 30 days, with a possible extension of another 30 days upon notification.

**12. Obligation to provide data protection training**

Service providers are obliged to conduct a documented training course on the data protection requirements according to HIPAA and GDPR every year.
ONCARE provides suitable materials or e-learning access for this purpose. Participation is digitally documented and must be proven to the Covered Entity on request.

**13. Secondary Use and Research Data**

Any use of PHI for research, analysis or marketing purposes by the Service Provider is prohibited unless:
- there is a documented consent ("Authorization") in accordance with 45 CFR §164.508,
- or a specific, HIPAA-compliant research data usage agreement has been concluded with ONCARE.

Internal secondary use (e.g., for quality assurance) is only permitted within the scope of HIPAA purpose limitation.

**14. Coordination with GDPR requirements**

With the simultaneous applicability of GDPR and HIPAA, ONCARE ensures that the stricter level of protection always applies. In particular, service providers undertake to:

- not to transfer data outside the EEA without appropriate Standard Contractual Clauses or sub-BAAs;
- Coordinate data subject rights from both jurisdictions (e.g., right to erasure under Art. 17 GDPR vs. retention obligations under HIPAA) in accordance with ONCARE.

**15. Supplemental State Data Protection Requirements (USA)**

In addition to the federal regulations under the Health Insurance Portability and Accountability Act (HIPAA), certain data processing is subject to supplemental or stricter data protection laws of individual US states. This applies in particular if affected users reside in one of these states, use our services from there or if personal data is processed by service providers or contractual partners based in these states.

The following federal privacy laws may be applied in addition or in priority, depending on the individual constellation:
- California: California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- New York: SHIELD Act
- Virginia: Virginia Consumer Data Protection Act (VCDPA)
- Colorado: Colorado Privacy Act (CPA)
- Connecticut: Data Privacy Act (CTDPA)
- Utah: Utah Consumer Privacy Act (UCPA)
- Illinois: Biometric Information Privacy Act (BIPA)
- Texas: Data Privacy and Security Act (TDPSA, effective 01.07.2024)
- Florida: Digital Bill of Rights (FDBR)

We are committed to complying with applicable federal regulations for all processing activities and to providing data subjects with comprehensive information on the application of these rights upon request. For certain states (e.g., California), we provide separate privacy notices upon request. Please contact us at **privacy@myoncare.com** if you would like to exercise your privacy-related rights under federal or state law.

**16. No Commercial Use of Portal User Personal Data**
Personal data of portal users (e.g. healthcare providers) is not used for research, marketing, or any other commercial purposes. ONCARE only processes fully anonymised technical usage data (e.g. aggregated login timestamps or system usage patterns) to improve the technical performance of the platform. These data do not contain any information that could be used to identify individual users and are not considered Protected Health Information (PHI) under the HIPAA Privacy Rule.

***