MYONCARE PATIENT APP – PRIVACY POLICY (EUROPE)

Version: February 2025

PRIVACY POLICY FOR EUROPE

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

For us at Oncare GmbH (hereinafter "**ONCARE"** or "**we**", **"us**", "**our**"), the protection of your privacy and all personal data relating to you during the use of the **app** is of great 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 core 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. This privacy policy explains 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 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.

In case of questions of interpretation or disputes, only the German version of the Privacy Policy shall be binding and authoritative.

DEFINITIONS

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

"**blockchain**" is another decentralized 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 based on 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 standardized treatment plan consisting of several scheduled care tasks, 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 app**" means the myoncare Progressive Web App application for patients who wish to use the services offered by ONCARE via the PWA App and not via 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 that uses 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.

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**.

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 from which information about their state of health precedes.

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.

myoncare PWA app

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 features 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 into the browser. The PWA is based on the technology of "React". "React" is open-source software for PWA applications.

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

Some of the myoncare app services cannot be used within the **myoncare PWA app**, see the description below for details. These are the following services or specifications:
- Chat with **healthcare providers**;
- Video;
- Security PIN codes;
- Activity data tracking (e.g. via AppleHealth, GoogleFit, Withings).

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

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, symptoms of illness 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.

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 **healthcare 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.

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 devices or pharmaceutical companies to fulfil legal security or vigilance purposes.

Reimbursement Data: Personal data required for the reimbursement process between your healthcare 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 about a particular internal or external situation, or data about care or health in general.

BLOCKCHAIN-TECHNOLOGY

Blockchain technology ("**blockchain**") (European Patent No. 4 002 787) is an optional service that is not mandatory. It is your **healthcare 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 that stores data from the application. 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, allowing transactions and changes of information to 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 is 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 would also change and the link to that block would 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. If all nodes (network nodes) attempt to synchronize their copies, it is detected that a copy has been modified, and the network deems that node to be faulty.

Our **blockchain** is a private **blockchain**. A private **blockchain** is decentralized. It is a so-called distributed ledger system (digital system for recording transactions), which functions as a closed database. Unlike public **blockchains**, which are "unauthorized," private **blockchains** are "authorized" because authorization is required to become a user. In contrast to public **blockchains**, which are publicly accessible to everyone, access to private **blockchains** is dependent on authorization in order to become a user. This structure makes it possible to take advantage of the security and immutability of blockchain technology while being data protection compliant and comply in particular with the regulations of the General Data Protection Regulation (GDPR). Private blockchain records can be edited, altered, or deleted; deletion in this context means that the reference value to the UUID (Universally Unique Identifier) in the database of the **healthcare provider** is deleted. In addition, the hash is anonymized in the blockchain database, with the result 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
- Patients-UUID
- Asset-UUID
- Hash of caretask and asset data.

(UUID: Universal Unique Identifier).

The data stored in the **blockchain** is 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 **healthcare provider** and on the patient's mobile phone. A backup copy of the patient key is encrypted and stored in the **healthcare provider**'s database, which can only be accessed by the patient.

When verifying consent to data protection, in the event that the **healthcare provider** wants to communicate with the patient, the system checks whether the patient has given consent to the **healthcare 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 agrees to the privacy policy, that interaction is stored on the **blockchain**. Every time it communicates with the patient, 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 **healthcare provider** achieves sufficient up-to-dateness with regard to the patient profile.

myoncare Portal:
If the **healthcare provider** decides to use 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 for the **healthcare provider** is carried out based on Art. 28 GDPR (Data Processing Agreement).

OPERATIONAL DATA PROCESSING

Applicable to all app users

You may provide us with certain personal information when you contact us to understand the features and usage of the **myoncare app**, in the event of a service request or in the case of support offers initiated by us (via telephone).

Service Staff
On behalf of the data controller (e.g., healthcare provider), we offer you assistance in completing questionnaires via telephone support (outbound calls) to optimize your digital patient care. Should you choose not to use this service, you are free to decline and object to telephone support.

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

- The personal data you have provided to your **healthcare 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**, the **data service provider** or the **company** via our **myoncare app** (e.g. information about medications taken, answers to questionnaires including disease- or condition-related information, diagnoses and therapies by healthcare professionals, planned and completed tasks).

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

Push Notifications and E-mails
As part of your support by 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, 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 informed about your tasks and important updates to best support your health.
- 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 the smooth receipt 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 the **myoncare app** is downloaded, the necessary information is transmitted to the app store provider. We have no control over 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.

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.

The app uses 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 detailed information about the scope, legal basis and purpose of data processing by Google as well as the storage period in the Google 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 if we are contacted by you (e.g. in the event of changes to the terms and conditions, necessary support, technical problems, assistance in completing questionnaires etc.).

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

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 it to secure our applications and to 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 any other information about the user that could identify them. The data processed by apilayer includes the patient's IP address and other details about the location. The legal basis for the use is Art. 6 para. 1 lit. f GDPR. The data will be deleted when the associated purpose for which it was collected no longer exists and there is no longer a legal obligation to store it. For more information about their privacy policy, please visit https://ipapi.com/privacy/ and

PROCESSING OF (TREATMENT) DATA

Applicable to app users who use the app with their healthcare provider

While using the **myoncare app**, your **healthcare provider** may enter your personal data into the **myoncare portal** in order to start **myoncare services** (e.g. create your patient file, providing an individual task, reminder to take medication, etc.). In addition, you and your **healthcare provider** can upload documents and files to the **myoncare app** and the **myoncare portal** and share them with each other. Your **healthcare provider** may upload a **privacy policy** for your information and define other consent requirements for you as a patient for which your consent must be given. The files are stored in a cloud database in Germany. Your **healthcare provider** may allow the sharing of such files with other **portal users** within its institution or other **healthcare providers** outside of his institution (consulting **healthcare provider**) for medical purposes. Other portal users do not have access to these files unless access is provided by your **healthcare provider**. Furthermore, your **healthcare provider** may instruct us to assist you via telephone in completing questionnaires (outbound calls). This is carried out solely at the direction of your **healthcare provider** and exclusively by authorized ONCARE employees.

We will use and process your data in accordance with what is set out in this **privacy policy**, as you give us your consent.

We process such personal data, including your health data, under an agreement with and in accordance with the instructions of your **healthcare provider** (data processing agreement). For the purposes of this data processing agreement, the **healthcare provider** is responsible for the processing of your personal data and health data within the meaning of applicable data protection laws as a data officer, 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 **healthcare 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 of healthcare professionals, planned and completed tasks.

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

Justification of processing treatment data: Your personal (treatment) data will be processed by your

healthcare 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 para. 2 lit. h GDPR for health data as data worthy of special protection as well as your consent pursuant to Art. 6 para. 1 lit. a and 9 para. 2 lit. a GDPR. The processing of data by ONCARE for your **healthcare provider** is also carried out on the basis of Art. 28 GDPR (order processing agreement).

Your **healthcare provider**, as a data officer, is responsible for obtaining your consent. 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**). Therefore, the refusal or revocation of consent to the processing of treatment data leads to a severe restriction of the functionality of the pp services and your **healthcare provider** can no longer support you via the **myoncare app**.

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 activity data processing, we will obtain your consent to the processing in advance. If the connection is established after you have given your consent, activity data collected by the **health app** will be made available to your **healthcare providers** for the purpose of providing additional, contextual information regarding 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 **healthcare providers** are not obliged to verify your activity data and do not have to give you any feedback regarding your activity data.
Activity data is shared with your affiliated **healthcare providers** every time the **myoncare app** is accessed. You can revoke your consent to share activity data at any time in the settings of the **myoncare app**. Please note that your activity data will not be shared from this point on. Activity data that has already been shared will not be deleted from the **myoncare portal** of your affiliated **healthcare providers**.

The processing of activity data falls under your own data responsibility.

Types of data: The type and scope of data transferred depend on your decision and the availability of this 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 processing activity data: Your activity data will be made available to your **healthcare providers** with whom you are connected for the purpose of providing additional, contextual information regarding your activity.

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

PROCESSING OF PRODUCT SAFETY DATA

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

The **myoncare app** is classified and marketed as a medical device according to the European medical device regulations. As the manufacturer of the app, we must 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.). In addition, the **myoncare app** allows you and your **healthcare provider** to communicate and collect personal data about certain medical devices or medicines used in your treatment. The manufacturers of such medical devices or medicinal products also have legal obligations regarding market surveillance (e.g. collection and evaluation of adverse reaction 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 (if possible after pseudonymization) to competent authorities, notified bodies or other data officers with supervisory obligations. In addition, we will store and transfer personal data in connection with medical devices and/or medicines if we receive notices from your **healthcare provider**, from you as a patient or from a third party (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 the manufacturer 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 medicinal product manufacturer is Art. 6 para. 1 lit. c, Art. 9 para. 2 lit. i GDPR in conjunction with the post-market monitoring obligations under the Medical Devices Act and the Medical Devices Directive (regulated as of 26 May 2021 in Chapter VII of the new Medical Devices Regulation (EU) 2017/745) and/or the Medicines Act.

CHANGES TO THE PRIVACY POLICY

Applicable to app users who use the app with their healthcare provider for reimbursement purposes

The **myoncare app** supports your **healthcare provider** in initiating standard procedures for reimbursement of costs for the health 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 **healthcare provider** for the transmission of this data to your paying unit (either its Association of Statutory Health Insurance Physicians and/or your health insurance company). This data processing is only an initial data transfer for the **healthcare provider** in order 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 **healthcare provider**. Your **healthcare provider** is the data officer of reimbursement data. ONCARE acts as a data processor on the basis of the data processing agreement with your **healthcare provider**.

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

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

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

PROCESSING OF OCCUPATIONAL HEALTH MANAGEMENT DATA

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

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 service providers** commissioned by the **company** (e.g. data analysts or research companies). Neither the **Company** nor any **data service provider** can assign such data to your identity. ONCARE recommends not to share any personal data during the use of **myoncare services** as part of occupational health management.

This means that ONCARE and all **data service 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 service provider** and in accordance with their instructions. For the purposes of this Agreement, the **company** or the **data service provider** is the data officer for the processing of your data for occupational health management purposes and ONCARE and any **data**

service providers engaged by the **company**, if any, are the 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 company health management data, which you enter into our **myoncare app**, will be used by the **company** (either directly or via a **data service provider**) in its occupational health management. We process this data for occupational health management as part of an agreement with and in accordance with the instructions of the **company** and/or a **data service provider** for its occupational health management. The transmission of this data for occupational health management is pseudonymized 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 para. 1 lit. a and Art. 9 para. 2 lit. a GDPR or another legal ground applicable to the **company**. The processing of data by ONCARE to the **company** (either directly or via a **healthcare provider** commissioned by your company) is also based on Art. 28 GDPR (Data Processing Agreement).
The **company,** as the data controller, is responsible for obtaining your consent if required by data protection regulations and for processing the data for occupational health management purposes in accordance with applicable data protection laws.

WHAT TECHNOLOGY IS USED BY THE MYONCARE APP?

E-mail 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 e-mail services can be used to organize the sending of e-mails. Sendgrid is used to send confirmation emails, transaction confirmations, and emails with important information related to requests. The data you enter for the purpose of receiving e-mails is 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 in to 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;
- Generation and sending of a report;
- Replace push notifications with emails for **PWA** (Progressive Web App) in the following cases:
    (i) if a Care Plan ends in one hour;
    (ii) if medication has been assigned;
    (iii) if the Privacy Policy has been updated;
    (iv) when an appointment is sent to patients and physicians, especially for the "video call" appointment type;
    (v) Any information relating to a **caretask** or if a **healthcare 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 outside of ONCARE's control. Matomo is initially disabled when you use our services. Only if you agree, your user behavior will be recorded anonymously. If deactivated, 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 Role;
- User geolocation;
- User-OS;
- Time that the user has used content;
- IP address;
- Sites visited via 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 passed on to 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, see: 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 analyze usage behavior. 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 is necessary to fulfil the intended purpose.

SECURE TRANSFER OF PERSONAL DATA

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

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

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 based on 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 during transmission.

GENERAL INFORMATION ON CONSENT TO DATA PROCESSING

Your consent also constitutes consent to data processing under data protection law. Before granting 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 pursuant to Art. 9 para. 1 GDPR may only take place if this is required by law 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 para. 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**.

DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

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

In certain cases, **other 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 data processors for personal data. These **service providers** are Google (Google Firebase), cloud storage providers and support serviceproviders.

Google Firebase is a "NoSQL database" that enables synchronization between your **healthcare 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 easier "horizontal" scaling compared to tabular/relational database management systems in a cluster of machines.
For this purpose, a pseudo-key of the **myoncare app** is stored in Google Firebase together with the corresponding **care plan**. The data transfer is pseudonymized for ONCARE and its service providers, which means that ONCARE and its other service providers cannot establish a relationship with you as a data subject. This is achieved by encrypting the data during the transfer between you and your **healthcare providers** or **company** (either directly or to any **data service provider**) and by using pseudo-keys instead of personal identifiers such as name or email address to track these transfers. Re-identification takes place as soon as the personal data has reached the account of your **healthcare providers** or **company** in the **myoncare portal** or your account in the **myoncare app**, after it has been verified by specific tokens.

Our cloud storage providers offer cloud storage in which the Firebase manager, which manages the Firebase URLs for the **myoncare portal**, is stored. In addition, these service providers provide the isolated server domain of the **myoncare portal**, in which your personal data is stored. It also hosts myoncare's video and file management services, which enable encrypted video conferences between you and your **healthcare provider** as well as the exchange of files. Access to your personal data by you and your **healthcare provider** is ensured by sending specific tokens. This personal data is encrypted during transfer and at rest and pseudonymized for ONCARE and its service providers. ONCARE 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, for example, if you have forgotten your password, want to change your stored e-mail address, etc. The necessary order processing agreements have been concluded with these service providers; furthermore, the employees entrusted with the processing of service requests were trained accordingly. Upon receiving your service request, a ticket number will be assigned to it.
If it is a service request regarding your account usage, the relevant information that you have provided to us when contacting us will be forwarded to one of the authorized employees of the external service. They 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, which is 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 display content from Instagram (provider: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland), such as images, videos, or posts. If you click on a linked Instagram post, you will be redirected to Instagram. During this process, Instagram may set cookies and process user data.
When you visit a page containing a linked Instagram post, your browser may automatically establish a connection to Instagram's servers. Instagram thereby receives 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 may associate the visit with your user account.
Privacy Policy:
https://privacycenter.instagram.com/policy

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

To provide our services, we may engage service providers located outside the European Union (third country). If data is transferred to a third country where the level of protection for personal data is deemed inadequate, we ensure that appropriate measures are taken in accordance with national and European law. If necessary, this includes the implementation of Standard Contractual Clauses between the processing parties.

The personal data collected by this **myoncare app** is not stored in the app stores. Personal data will only be transferred to third countries (outside the European Union or the European Economic Area) 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** takes place via Google Firebase. The Google Firebase server is hosted in the European Union. However, as described in the Google Firebase Terms of Use, short-term data transfers to countries in which Google or its service providers are located are possible; for certain Google Firebase services, data is only transferred to the USA, unless 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. 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 integrate content from Instagram, provided by Meta Platforms Ireland Ltd. If you click on a linked Instagram post, it is possible that 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 recognizes an adequate level of data protection for transfers to the USA. However, data may also be transferred to countries for which there is no adequacy decision by the European Commission. In such cases, additional protective measures may be required, although their effectiveness cannot always be fully 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.

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

DURATION OF STORAGE OF PERSONAL DATA

We will retain your personal data for as long as it is needed for the purpose for which it is processed. Please note that numerous retention periods require the continued storage of personal data. This applies especially but not limited 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 **healthcare provider** based on the legal provisions. In addition, and only if your **healthcare 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. If there are no other retention obligations, the personal data will be 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 litigation arises and we use evidence within the statutory limitation periods, which can be up to 30 years; the regular limitation period is three years.

OBLIGATION TO PROVIDE PERSONAL DATA

Various personal data are necessary for the establishment, execution 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 above. In certain cases, personal data must also be collected or made available in accordance with the legal provisions. Please note that without providing this personal data, it is not possible to process your request or fulfil the underlying contractual obligation.

ACCESS

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 given various permissions to access certain functions of the device. If applicable, we will list them in order of the operating system (Android or iOS) according to the "basic conditions".
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 the functionality of document download 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.

Turn off 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 / Access to Mobile Data
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 necessary to ensure the functionality of disabling document downloads over mobile data.

Accessing the camera
Camera access is required for scanning QR codes as well as for 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 necessary to view received files from your connected portal users.

We use push notifications, which are messages that are sent to your mobile device as a service of the **myoncare app** via services such as Apple Push Notification Service or 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.

AUTOMATED DECISIONS IN INDIVIDUAL CASES

We do not use purely automated processing to make decisions.

YOUR RIGHTS AS A PERSON CONCERNED

We would like to inform you about your rights as a data subject. These rights are set out in Articles 15 – 22 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, 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 ask us to 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 for 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 if we process your personal data on the basis of your consent. We will continue to provide our services if they are not dependent on withdrawn consent.

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

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

DATA PROTECTION SUPERVISOR

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

AGE RESTRICTION OF THE APPLICATION

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

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 meet legal requirements, to comply with technical and economic developments, or to meet 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 case of questions of interpretation or disputes, only the German version of the Privacy Policy shall be binding and authoritative.

ONCARE GmbH

Mailing address

Balanstraße 71a

81541 Munich, Germany

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Contact information of the Data Protection Officer
privacy@myoncare.com

Last updated on February 20, 2025.
* * * *

U.S. PRIVACY POLICY

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

This Privacy Policy describes how your personal and medical information may be used and shared, and how you can access that information. Please read this Privacy Policy carefully. In this privacy policy, you will learn why and how ONCARE processes your personal health data provided to us if you decide to use the myoncare app.

For us at Oncare GmbH (hereinafter referred to as "**Oncare (ONCARE** or "**we**", "**us**", "**our**"), the protection of your privacy and the personal data concerning you when using the myoncare app is of great relevance and importance. We are aware of the responsibility that arises from your trust in providing and storing 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 core of our ethical understanding as a company.

Any information we hold that is provided by your **healthcare providers** is **Protected Health Information (PHI)** and/or other medical information. These are protected by certain laws, such as the U.S. Health Insurance Portability and Accountability Act (**HIPAA).** We have a legal obligation to protect the privacy and security of protected health information. We constantly strive to protect health information through administrative, physical, and technical means, and otherwise comply with applicable federal and state laws.

The use and disclosure of such **PHIs** is in accordance with applicable privacy policies and applicable laws. To understand in more detail how we process and share these **PHIs**, you should read this **Privacy Policy** carefully**.** Please read the Privacy Policy carefully to ensure that you understand each provision. After reading the Privacy Policy, you 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. We guarantee the rights and obligations described in this Privacy Policy. We use and process your data in accordance with the provisions of this privacy policy.

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.

DEFINITIONS

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

"blockchain technology" The myoncare system contains an additional database in which the data of all installations is stored.

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

"**covered entity**" means a health plan, health care clearinghouse, or healthcare provider that submits health information in electronic form in connection with a transaction that falls under HIPAA.

"**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.

"**EU General Data Protection Regulation**". The General Data Protection Regulation (GDPR) is a European data protection law. The regulation came into force on 25 May 2018 and aims to harmonize data protection across all member states and give citizens more control over their personal data. The GDPR applies to all companies and organizations that operate in the EU or process personal data of EU citizens, regardless of whether the company is located inside or outside the EU. The GDPR also applies to you as a US citizen because Oncare is based in Germany.

"**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 standardized treatment plan that 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.

"**health information**" means all information, including genetic information, whether recorded orally or in any form or on any medium, and which
- processed or transferred by a healthcare provider, health plan, health authority, employer, life insurer, school or university, or health clearing house; and
- relates to the past, present or future physical or mental health of a person or any health condition in connection with medical treatment of the person, as the case may be;
- the past, present or future fee remuneration for a person's health care. "**Protected Health Information**" or **"PHI"** means individually identifiable health information that

(i) is transmitted via electronic media;
(ii) are maintained in electronic media; or
(iii) transmitted or maintained in any other form or medium.

"**Health Insurance Portability and Accountability Act**," The Health Insurance Portability and Accountability Act of 1996 (**HIPAA)** is a U.S. federal law that provides for the creation of national standards to protect patients' sensitive health information from unauthorized disclosure without their consent or knowledge. The HIPAA requirements apply to the use and disclosure of health information of individuals by institutions subject to the HIPAA Act. These individuals and organizations are referred to as "covered entities."

"**myoncare PWA App**" means the myoncare Progressive Web App application for patients who wish to use the services offered by ONCARE via the PWA App 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.

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

"**ONCARE**" or "**we**" means ONCARE GmbH, based in 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 or employee and user of the myoncare app, which describes how we collect, use and store your personal data and informs you of your rights.

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

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

COMPLIANCE WITH LAWS

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**.

ONCARE is a "business associate" within the meaning of **HIPAA** that provides services and health plans to **healthcare providers** referred to as "covered entities" within the meaning of **HIPAA**; ONCARE concludes business partner agreements with these covered companies. ONCARE will only process and share the **PHIs** under the terms of the Agreements and **HIPAA**.

We are required by U.S. law to maintain the privacy and security of your protected health information.

We are required by U.S. law to follow laws designed to protect the privacy and security of protected health information. We will inform you immediately if a breach (so-called data breach) occurs that could have endangered the privacy or security of (health) information.

We must comply with the obligations and content described in this Privacy Policy and provide you with a copy of the Privacy Policy upon request.

No identifiable personal (health) information will be sold.

We will not use or share your information other than as described here, unless you tell us that we are allowed to do so.

U.S. Privacy Policy, U.S. federal and state laws may impose additional restrictions on the sharing of your health information in connection with medical treatment for drug or alcohol abuse, sexually transmitted diseases, genetic information, or mental health treatment programs. If relevant laws apply, we will obtain your consent before sharing or processing this data.

WHAT IS PERSONAL DATA WITHIN THE MEANING OF THE GDPR

We process your personal data in accordance with the applicable legal provisions on the protection of personal data, in particular the EU General Data Protection Regulation and the country-specific laws that apply to us. 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.

"**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 or mental health of a natural person, including the provision of health services that reveal information about their health status.

Data is considered "**anonymous"** if no personal reference to the person/user can be established. In contrast, "**pseudonymized**" data is data in which personal reference or personal data is replaced by one or more artificial identifiers or pseudonyms, but which can generally be reidentified by the identifier key (within the meaning of Art. 4 No. 5 GDPR).

myoncare PWA-App

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 features 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 into 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**, patients need a computer or smartphone and an active internet connection. There is no need to download an app.

Some of the **myoncare app** services cannot be used within the **myoncare PWA**, see the description below for details. These are the following services or specifications:

- Chat with **healthcare providers**;
- Video;
- Security PIN codes;
- Activity data tracking (e.g. via AppleHealth, GoogleFit, Withings).

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

WHAT PERSONAL DATA IS USED WHEN USING THE MYONCARE APP

We use and share your health information for usual business activities that fall into the categories of treatment and healthcare under the law. 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 enter personal data such as name, age, height, weight, indication, symptoms of illness and other information in connection with your treatment (e.g. in a care plan) with the support of the **myoncare app**. Information related to your treatment includes, but is not limited to: information about medications taken, questionnaire responses including disease- or condition-related information, diagnoses and therapies provided by your **healthcare provider** , planned and completed tasks).

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

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 meet legal security or vigilance objectives.

Reimbursement Information: Personal data required for the reimbursement process between your myoncare **healthcare provider** and your health insurance company.

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

BLOCKCHAIN-TECHNOLOGY

Blockchain **technology** ("**Blockchain**") (European Patent No. 4 002 787) is an optional service that is not mandatory. It is up to your **healthcare 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 that stores data from the application. 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, allowing transactions and changes of information to 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 is 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 would also change and the link to that block would be lost. If all nodes (network nodes) attempt to synchronize their copies, it is detected that a copy has been modified, and the network deems that node to be faulty. 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. It is a so-called distributed ledger system (digital system for recording transactions), which functions as a closed database. Unlike public

blockchains, which are "unauthorized," private **blockchains** are „authorized" because authorization is required to become a user. In contrast to public **blockchains**, which are publicly accessible to everyone, access to private **blockchains** is dependent on authorization in order to become a user. This structure makes it possible to take advantage of the security and immutability of **blockchain technology** while being data protection compliant, and in particular to comply with the regulations of the General Data Protection Regulation (**GDPR**). Private blockchain records can be edited, altered, or deleted; deletion in this context means that the reference value to the UUID (Universally unique identifier) in the database of the **healthcare provider** is deleted. In addition, the hash is anonymized in the blockchain database, with the result 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:

- Patients-UUID
- Institutions/Leistungserbinger UUID
- Asset-UUID
- Hash of **caretask** and asset data.

(*UUID: Universal Unique Identifier*).

The data stored in the **blockchain** is 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 **healthcare provider** and on the patient's mobile phone. A backup copy of the patient key is encrypted and stored in the **healthcare provider**'s database, which can only be accessed by the patient.

When verifying consent to data protection, in the event that the **healthcare 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 agrees to the privacy policy, that interaction is stored on the **blockchain**. Every time it communicates with the patient, 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 recognizes if the patient profile does not synchronize or match the profile on the mobile phone by comparing the hash of the patient profile in the **blockchain**. In this way, the **healthcare provider** achieves sufficient up-to-dateness with regard to the patient profile.

myoncare Portal:
If the **healthcare provider** decides to use 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 **healthcare provider** is carried out on the basis of Art. 28 GDPR (order processing agreement).

OPERATIONAL DATA PROCESSING

Applicable to all app users

You may provide us with certain personal information when you contact us to understand or discuss the features and use of the app, in the event of a service request or in the case of support offers initiated by us (via telephone).

Service Staff
On behalf of the data controller (e.g., healthcare provider), we offer you assistance in completing questionnaires via telephone support (outbound calls) to optimize your digital patient care. Should you choose not to use this service, you are free to decline and object to the telephone support.

In the event of a service request or an outbound call, the following personal data can also be viewed by authorized ONCARE employees:
- the personal data that you have provided to your **healthcare provider** via our app (e.g. name, date of birth, profile picture, contact details);
- the health information that you have provided to your **healthcare provider**, the **data service provider** or the company via our **myoncare app** (e.g. information about medications taken, responses to questionnaires including disease-related or condition-related information, diagnoses and therapies by healthcare professionals, planned and completed tasks).

Authorized ONCARE employees who may access the database of your **healthcare provider**, **data service provide**r or **company** for the purpose of processing a service request are contractually obliged to keep all personal data strictly confidential.

Important Explanations of Push Notifications and Emails

As part of your support by 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 informed about your tasks and important updates to best support your health.
- 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 the smooth receipt 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 the **myoncare app** is downloaded, the necessary information is transmitted to the app store provider. We have no control over 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**.

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.

The app uses 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 detailed information about the scope, legal basis and purpose of data processing by Google as well as the storage period in the Google Privacy Policy.

In our organization, 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. Your personal data and health data that you enter into our **myoncare app** will be made available to your **healthcare provider** and/or **company** either directly or via a **data service provider** (depending on the type of use of the **myoncare tools**).

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

IP GEOLOCATION

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 it to secure our applications and to 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 any other information about the user that could identify them. The data processed by apilayer includes the patient's IP address and other details about the location. The legal basis for their use is Art. 6 (1) (f) GDPR. The data will be deleted when the associated purpose for which it was collected no longer exists and there is no longer a legal obligation to store it. For more information on their privacy policy, please see https://ipapi.com/privacy/ and Privacy Policy | Geoapify location platform.

PROCESSING OF (TREATMENT) DATA

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

While using the myoncare app, your **healthcare provider** enters your personal data into the myoncare portal in order to start myoncare services (e.g. create your patient file, provision of an individual care plan, reminder to take medication, etc.). In addition, you and your **healthcare provider** can upload documents and files to the **myoncare app** and the **myoncare portal** and share them with each other. Your **healthcare provider** may upload a privacy policy for your information and define other consent requirements for you as a patient for which your consent must be given. The files are stored in a cloud database in Germany. Your **healthcare provider** may allow the sharing of such files with other **Portal Users** within its institution or other **healthcare providers** outside of his institution (consulting healthcare provider) for medical purposes. Other portal users do not have access to these files unless access is provided by your **healthcare provider**. Furthermore, your **healthcare provider** may instruct us to assist you via telephone in completing questionnaires (outbound calls). This is carried out solely at the direction of your **healthcare provider** and exclusively by authorized ONCARE employees.

We use and process your health information only for the operational activities permitted by HIPAA and other federal laws.

We process such personal data, including your health data, under an agreement with and in accordance with the instructions of your **healthcare provider** (data processing agreement). For the purposes of this data processing agreement, the **healthcare provider** is responsible for the processing of your personal data and health data within the meaning of applicable data protection laws as a data controller, 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 **healthcare 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.

PROCESSING OF ACTIVITY DATA

Only applicable if you agree to and activate the 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**"). If the connection is established after you have given your consent, activity data collected by the Health Application will be made available to your **healthcare providers** for the purpose of providing additional, contextual information regarding your activity. In order to enable activity data processing, we will obtain your consent to the processing in advance. 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 **healthcare providers** are not obliged to verify your activity data and do not have to give you any feedback regarding your activity data.

Activity data is shared with your affiliated **healthcare providers** every time the **myoncare app** is accessed. You can revoke your consent to share activity data at any time in the settings of the **myoncare app**. Please note that your activity data will not be shared from this point on. Activity data that has already been shared will not be deleted from the **myoncare portal** of your affiliated **serv healthcare providers**.

The processing of activity data falls under your own data responsibility.

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

Purpose of processing activity data: Your activity data will be made available to your **healthcare providers** with whom you are connected for the purpose of providing additional, contextual information regarding your activity.

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

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 according to the European medical device regulations. As the manufacturer of the app, we must 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.). In addition, the **myoncare app** allows you and your **healthcare provider** to communicate and collect personal data about certain medical devices or medicines used in your treatment. The manufacturers of such medical devices or medicinal products also have legal obligations regarding market surveillance (e.g. collection and evaluation of adverse reaction reports).

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

Processing of product safety data: We will store and evaluate all personal data related to our legal obligations as a manufacturer of a medical device and transmit such personal data (if possible after pseudonymization) to competent authorities, notified bodies or other data controllers with monitoring obligations. In addition, we will store and transfer personal data in connection with medical devices and/or medicines if we receive notices from your **healthcare provider**, from you as a patient or from a third party (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 the manufacturer to comply with its legal obligations on product safety .

GDPR rules

ONCARE is the data controller for 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 medicinal product manufacturer is Art. 9 para. 2 lit. i GDPR in conjunction with the monitoring obligations existing after placing on the market under the Medical Devices Act and the Medical Devices Directive (regulated as of 26 May 2021 in Chapter VII of the new Medical Devices Regulation (EU) 2017/745) and/or the Medicines Act.

PROCESSING OF OCCUPATIONAL HEALTH MANAGEMENT DATA

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

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 service providers** commissioned by the company (e.g. data analysts or research companies). Neither the **company** nor any **data service provider** can assign such data to your identity. ONCARE recommends not to share any personal data during the use of **myoncare services** as part of occupational health management.
This means that ONCARE and all **data service 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 the **company** and/or a **data service provider** and in accordance with their instructions. For the purposes of this Agreement, the Company is the data officer responsible for the processing of your Occupational Health Management Data and ONCARE and any **data service providers** engaged by your **company**, if any, are the 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.

Data processing: We process your company health management data in order to be able to provide our **myoncare services** for the **company** and for you. Your occupational health management data, which you enter in our **myoncare app**, will be used by the **company** (either directly or via a **data service provider**) as part of occupational health management. We process this personal data under an agreement with and in accordance with the instructions of your **healthcare provider**. The transmission of this treatment data is pseudonymized and encrypted. To exercise your rights as a data subject, please contact your **service provider**.

GDPR rules

Your data for occupational health management 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 para. 1 lit. a and Art. 9 para. 2 lit. a **GDPR** or another norm applicable to the **company**. The processing of data by ONCARE to the **company** (either directly or via a **service provider** commissioned by the **company**) is also based on Art. 28 **GDPR** (Data Processing Agreement).

The **company,** as the data officer, is responsible for obtaining your consent if required by data protection regulations and for processing the data for occupational health management purposes in accordance with applicable data protection laws.

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 any current version of the internet browser Chrome, Firefox or Safari.

E-mail 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 e-mail services can be used to organize the sending of e-mails. Sendgrid is used to send confirmation emails, transaction confirmations, and emails with important information related to requests. The data you enter for the purpose of receiving e-mails is 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 in to the web application for the first time;
- Workflow to reset the password for the web application;
- Create an account for the patient application;
- Reset the password for the patient application;
- Generation and sending of a report;

- Replace push notifications with emails for PWA (Progressive Webapp) in the following cases:
(i) If a Care Plan ends within one day;
(ii) if medication has been assigned;
(ii) when the Privacy Policy has been updated;
(iv) when an appointment is sent to patients and physicians, especially for the "video call" appointment type;
(v)All information about a **caretask** or when a **healthcare 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 outside of ONCARE's control. Matomo is initially disabled when you use our services. Only if you agree, your user behavior will be recorded anonymously. If deactivated, a "persistent cookie" will be stored, provided that 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 Role;
- User geolocation;
- Browser;
- User-OS;
- IP address;
- Sites visited via web / PWA (for more information, see the section on PWA in this Privacy Policy);
- buttons that the user clicks on in the **myoncare portal**, in the **myoncare app** and in the **myoncare PWA**;
- time that the user has used content.
The information generated by the cookie will not be passed on to 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, see: 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 analyze usage behavior. 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 is necessary to fulfil the intended purpose.

SECURE TRANSFER OF PERSONAL DATA

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

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

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 during transmission.

We will only share information and data about you if required to do so by state or U.S. federal law; this includes requests from the Department of Health and Human Services if the agency wishes to verify compliance with U.S. federal law. We may also process and share your health data in order to:

- compliance with federal, state or local laws;

- To provide support for public health activities, such as illness or the use of medical equipment;
- to provide authorities with information to protect victims of abuse or neglect;
- Compliance with federal and state health oversight activities, such as fraud investigations;
- To enforce law enforcement or court orders, subpoenas, or other related sovereign actions;
- Conducting research on internal review protocols to ensure a balance between privacy and research needs;
- Averting a serious threat to health or safety.

GENERAL INFORMATION ON CONSENT TO DATA PROCESSING

Your consent also constitutes consent to data processing under data protection law. Before granting 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.

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**.

GDPR rules

Processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR may only take place if this is required by law 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 para. 2 GDPR.

DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

In our organization, we ensure that only those individuals are authorized to process personal data that are necessary to fulfill their contractual and legal obligations. Your personal data and health data that you enter in our **myoncare app** will be made available to your **healthcare provider** and/or **company** either directly or via a **data service 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 data processors for the 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 **healthcare 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 easier "horizontal" scaling compared to tabular/relational database management systems in a cluster of machines.

For this purpose, a pseudo-key of the **myoncare app** is stored in Google Firebase together with the corresponding care 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 during the transfer between you and your **healthcare provider** or **company** (either directly or to any **data service provider**) and by using pseudo-keys instead of personal identifiers such as name or email address to track these transfers. Re-identification takes place as soon as the personal data has reached the account of your **healthcare provider** or **company** in the **myoncare portal** or your account in the **myoncare app**, after it has been verified by specific tokens.

Our cloud storage providers offer a range of cloud storage services in which the Firebase manager, which manages the Firebase URLs for the **myoncare portal**, is stored. In addition, these service providers provide the isolated server domain of the **myoncare portal**, in which your personal data is stored. It also hosts myoncare's video and file management services, which enable encrypted video conferences between you and your **healthcare provider** as well as the exchange of files. Access to your personal data by you and your **healthcare provider** is ensured by sending specific tokens. This personal data is encrypted during transfer and at rest and pseudonymized for ONCARE and its service providers. ONCARE 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, for example, if you have forgotten your password, want to change your stored e-mail address, etc. The necessary order processing agreements have been concluded with these service providers; furthermore, the employees entrusted with the processing of service requests were trained accordingly. Upon receiving your service request a ticket number will be assigned to it.

If it is a service request regarding your account usage, the relevant information that you have provided to us when contacting us will be forwarded to one of the authorized employees of the external service. They will then contact you.

Otherwise, it will remain 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 which 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 display content from Instagram (provider: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland), such as images, videos, or posts. If you click on a linked Instagram post, you will be redirected to Instagram. During this process, Instagram may set cookies and process user data.

When you visit a page containing a linked Instagram post, your browser may automatically establish a connection to Instagram's servers. Instagram thereby receives 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 may associate the visit with your user account.
Privacy Policy:
https://privacycenter.instagram.com/policy

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

To provide our services, we may engage service providers located outside the European Union (third country). If data is transferred to a third country where the level of protection for personal data is deemed inadequate, we ensure that appropriate measures are taken in accordance with national and European law. If necessary, this includes the implementation of Standard Contractual Clauses between the processing parties.

Personal data will only be transferred to third countries 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** takes place via Google Firebase. The Google Firebase server is hosted in the European Union. However, as described in the Google Firebase Terms of Use, short-term data transfers to countries in which Google or its service providers are located are possible; for certain Google Firebase services, data is only transferred to the USA, unless processing takes place in the European Union or the European Economic Area. Unlawful access to your data is prevented by end-to-end encryption and secure access tokens. Our 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.

We integrate content from Instagram, provided by Meta Platforms Ireland Ltd. If you click on a linked Instagram post, it is possible that 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 recognizes an adequate level of data protection for transfers to the USA. However, data may also be transferred to countries for which there is no adequacy decision by the European Commission. In such cases, additional protective measures may be required, although their effectiveness cannot always be fully guaranteed.

GDPR - Rules

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

DURATION OF STORAGE OF PERSONAL DATA IN ACCORDANCE WITH THE GDPR

We will retain your personal data for as long as it is needed 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 (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).
In addition, and only if your **healthcare 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. Please note that ONCARE is also subject to retention obligations that are contractually agreed with your **healthcare provider** on the basis of the legal provisions. If there are no other retention obligations, the personal data will be 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 litigation arises and we use evidence within the statutory limitation periods, which can be up to 30 years; the regular limitation period is three years.

TRANSFERS OF PERSONAL DATA

Various personal data are necessary for the establishment, execution 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 point above. In certain cases, personal data must also be collected or made available in accordance with the legal provisions. Please note that without providing this personal data, it is not possible to process your request or fulfil the underlying contractual obligation.

ACCESS RIGHTS

In order for the **myoncare app** to work on your device, the app must be given various permissions to access certain functions of the device. For all devices, regardless of the operating system used, it is necessary to grant the app certain permissions, which we call "basic access rights". If applicable, we will list them in order of the operating system (Android or iOS) according to the "basic conditions". 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.

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 the functionality of document download 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.

Turn off 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 / Access to Mobile Data
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 necessary to ensure the functionality of disabling document downloads over mobile data.

Access to the camera
Camera access is required for scanning QR codes as well as for video consultations.

Access to 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.

Access to web browsers
This is necessary to view received files from your connected portal users.

We use push notifications, which are messages that are sent to your mobile device as a service of the **myoncare app** via services such as Apple Push Notification Service or 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.

AUTOMATED DECISIONS IN INDIVIDUAL CASES IN ACCORDANCE WITH THE GDPR

We do not use purely automated processing to make decisions.

YOUR HIPAA RIGHTS

Under **HIPAA**, you have the following rights:

- Viewing and copying certain portions of your health information. You can request that your health data be made available to you in electronic form. A copy or summary of your health information will be provided to you, usually within 30 days of your request. A reasonable processing fee may be charged.

- You can request that the contents of your health information be changed if you believe that the health information is incorrect or incomplete. You can request correction of health information if you believe it is inaccurate or incomplete.

- Establish mandatory disclosures of your health information for the past six years, with restrictions on treatment, reimbursement, and treatment. A reasonable processing fee may be charged.

- You can request that certain health information that includes treatment, royalty payments or other medical topics may not be used or shared.

- You may request a paper copy of the Privacy Policy at any time, even if you have agreed to receive the notice only electronically.

- File a complaint with the competent authority if you believe that your data protection rights have been violated. You may file a complaint with the U.S. Department of Health and Human Services by mailing a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, by phone at 1-800-368-1019 (toll-free) or 1-800-537-7697 (TTD), or by visiting https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf .

Many U.S. states have enacted their own laws to protect patients' rights, which apply to patients of physicians and/or hospitals and other healthcare facilities. Some of these U.S. states require physicians to provide a copy of these patient rights to their patients.

YOUR RIGHTS AS A DATA SUBJECT UNDER GDPR

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

Right to information (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, 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 ask us to 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.

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 for 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 if we process your personal data on the basis of your consent. We will continue to provide our services if they are not dependent on withdrawn consent.

To exercise these rights, please contact your **healthcare provider** or **company** in the first instance or contact us at: privacy@myoncare.com . We will require you to provide sufficient proof of your identity to ensure that your rights are protected and that your personal data will only be disclosed to you and not to 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.

SUBMIT A COMPLAINT

If you believe that your privacy has been violated by ONCARE, you may file a complaint with us and the U.S. Secretary of Health and Human Services in Washington, D.C. There are no disadvantages for you for filing a complaint. To file a complaint or receive further information, please use the following contact options:

Phone: +49 (0) 89 4445 1156

E-mail: privacy@myoncare.com

Address: Balanstraße 71a
81541 Munich, Germany

Re: Complaint

To file a complaint with the U.S. Department of Health and Human Services, write to 200 Independence Ave., S.W., Washington, D.C. 20201 or call 1-800-368-1019 (toll-free) or 1-800-537-7697 (TTD) or file an online complaint at https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

DATA PROTECTION OFFICER ACCORDING TO GDPR

Our data protection officer is available to answer all data protection questions at privacy@myoncare.com .

AGE RESTRICTION OF THE APPLICATION

A minimum age of 18 years is required to use the **myoncare app**. If you are under 18 years of age, your parent or guardian must provide the consent to privacy required to use the app.

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 meet legal requirements, to comply with technical and economic developments, or to meet 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).

ONCARE GmbH

Mailing address

Balanstraße 71a
81541 Munich, Germany

T | +49 (0) 89 4445 1156

E | privacy@myoncare.com

Contact information of the Data Protection Officer
privacy@myoncare.com

Last updated on February 20, 2025

* * * *