PRIVACY POLICY FOR EUROPE

Welcome to myoncare, the digital health portal for efficient and demand-oriented patient care.
For us at Oncare GmbH (hereinafter referred to as "**ONCARE"** or "**we**", **"us**", "**our**"), the protection of your privacy and your personal data processed during the use of the myoncare portal is of great importance. We are aware of the responsibility that arises from the provision and storage of your personal data in the myoncare portal. 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 the applicable legal provisions on the protection of personal data, in particular the EU General Data Protection Regulation ("**GDPR")** and the country-specific laws that apply to us. In this Privacy Policy, you will find out why and how **ONCARE** processes your personal data that we collect from you or that you provide to us when you decide to use the myoncare portal. In particular, you will find a description of the type of personal data we collect and process, as well as the purpose and basis on which we process the personal data; furthermore, you will find the rights to which you are entitled.

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

In 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 (your patient).

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

"Careplan provider" means you or any other service provider or third party (e.g. medical device manufacturer, pharmaceutical company) who makes Care Plans available to other Portal users via the myoncare Store or other means of data exchange.

"Careplan user" means you or any other service provider (Portal User) who uses a Care Plan ("Pathway") for the treatment of its registered Patients.

"Pathway" is a standardized treatment plan consisting of several scheduled care tasks, 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 themselves.

"**healthcare provider**" means you or any other physician, clinic, healthcare facility or other healthcare professional acting alone or on behalf of you or another physician, clinic or healthcare facility (intended User).

"**myoncare app**" refers to the mobile myoncare application for patients who wish to use the services offered by ONCARE via app.

"**myoncare store"** is the platform operated by **ONCARE** that provides digital care concepts (care plans) for the treatment of your registered patients via the myoncare portal.

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

"myoncare PWA 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 intended for professional use by portal users and serves as an interface between portal users and patients as app users.

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

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

"**Portal User**" means you or any other service provider using the web-based myoncare Portal.

"**Patient Privacy Policy**" means the privacy policy that describes the collection, use and storage of the personal (health) information of patients using the myoncare App. According to the terms of use, our offer is only aimed at patients aged 18 and over. Accordingly, no personal data of children and adolescents under the age of 18 is stored and processed.

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

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

PROCESSING OF (TREATMENT) DATA

Oncare GmbH, a company registered with the District Court of Munich under the registration number 219909 with its registered office at Balanstraße 71a, 81541 Munich, Germany, offers and operates the interactive web portal myoncare Portal (for healthcare professionals) and the mobile application myoncare App (for patients) as access to the myoncare services. This **privacy policy** applies to all personal data processed by ONCARE in connection with the use of the myoncare portal. For the use of the myoncare app by patients, you will find a separate privacy policy for patients **here**.

WHAT IS PERSONAL DATA

"**Personal data**" means any information that allows a natural person to be identified. This includes but is not limited to your name, birthday, address, 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 healthcare services, from which information about his or her 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. (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 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 and logging in to our **myoncare portal**, when contacting us about issues with the portal or when otherwise interacting with us for the purpose of using the portal.

Treatment data: You collect personal data of your patients, such as name, age, height, weight, indication,

symptoms of illness and other information in connection with the treatment of your patients (e.g. in a care plan) in the **myoncare portal**. Activity data of your connected patients is made available to you in your **myoncare portal**.

Commercial store data: Personal data that is processed by us in the case of using the **myoncare store**, either in the context of authorship of care plans or the purchase of care plans. The use of the **myoncare store** will require the processing of your name and other contact information as well as payment details (payment information only if the care plan is subject to a fee).

Activity data: Personal data that is processed by us when an **app user** connects the **myoncare app** to a health application (e.g. AppleHealth, GoogleFit, Withings). Activity data of your connected patients is made available to you in your **myoncare portal**.

Commercial and non-commercial research data:
We process your personal data in anonymized/pseudonymized form 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 information may be processed in case you report an incident to fulfill legal security or vigilance purposes of medical device or pharmaceutical companies.

Reimbursement data: Personal data required for the reimbursement process.

BLOCKCHAIN-TECHNOLOGY

Blockchain technology ("**blockchain**") (European Patent No. 4 002 787) is an optional service that is not mandatory. It is up to you, the **healthcare provider**, to decide to use the blockchain solution. The **blockchain** is based on Hyperledger Fabric's technology. Hyperledger Fabric is 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 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 determined that the modified copy has been modified, and the network deems that node to be faulty. This technical process prevents unauthorized people 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 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 detects if the patient's 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's profile.

myoncare portal:
If the **healthare 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 based on Art. 28 GDPR (order processing agreement).

OPERATIONAL DATA PROCESSING

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

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

Your personal data that you have provided to us for registration and/or login to our portal (e.g. name, date of birth, profile picture, contact details).

Authorized ONCARE employees who may access your database for the purpose of processing a service request are contractually obligated to keep all personal information 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 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 that you are always informed about your tasks and important updates to optimally support your care.
- Emails are a reliable way to ensure that important information reaches you, even when push notifications are disabled.

Your options for action:

- If you do not want to receive push notifications, you can deactivate them in the settings of the **myoncare app**.
- Please ensure that your email address is accurate and up to date to ensure 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 processing operational data, ONCARE acts as a data controller responsible for the lawful processing of your personal data.

Types of Data: e-mail address, date of birth, date of registration, your IP address, pseudo-keys generated by the Portal.

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.

Purpose of processing operational data: We use the operational data to maintain the functionalities of the **myoncare portal** and to contact you directly if necessary or on your initiative (e.g. in the event of changes to terms of use, necessary support, technical problems, etc.). Furthermore, personal data (e-mail address) is required and processed within the framework of two-factor authentication every time you log in to the **myoncare portal**.

Justification of processing: The processing of operational data is justified based on 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 portal**.

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

PROCESSING OF TREATMENT DATA

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

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

It is possible to create further consent requirements for the patient, for which the patient must give consent in order to connect to the website.

An uploaded privacy policy will be displayed to every patient who connects to the website. All declarations of consent must be documented in the uploaded privacy policy. Once a privacy policy has been uploaded, it can only be replaced by a new version but cannot be deleted. The files are stored in a cloud database in Germany. You can allow the sharing of such files with other **portal users** within your institution for medical purposes. Other **portal users** do not have access to these files.

Furthermore, you may involve a **healthcare provider** outside your facility (consulting healthcare provider) in the treatment of your patients, provided you believe that an additional expert opinion would benefit the treatment.

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

We process such personal data, including the patient's health data, under an agreement with you and in accordance with your instructions. Please only process your patients' data if you have obtained the required data consent from these patients. ONCARE acts as a data processor in accordance with the separate data processing agreement, which we have concluded with you based on Art. 28 GDPR.

PROCESSING OF COMMERCIAL STORE DATA

Only applicable if you use the myoncare Store as a Careplan user.

The **myoncare store** is integrated into the **myoncare portal** and offers the purchase of care plans. After registering with the **myoncare portal**, you can connect to the **myoncare store** using your login details. You can use the **myoncare store** to purchase care plans as a user.

Data of the careplan user:

The data of the **careplan user**, which the **myoncare Store** processes during its use, is processed for the conclusion of a license agreement with the **careplan provider** – in this case ONCARE – and, if a fee is due, for the processing and control of the payment transaction between **the careplan provider** – in this case ONCARE – and **the careplan user**.

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

Processing of commercial store data: Personal data that is processed by us in the case of using the **myoncare store** as part of the purchase of care plans. In addition, the payment data (if a usage fee is charged) will be forwarded to the **careplan provider**.

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

PROCESSING OF ACTIVITY DATA

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

Myoncare tools offer **app users** the option of connecting the **myoncare app** to certain health apps (e.g.

AppleHealth, GoogleFit, Withings) ("**Health App**"), provided that these are used by the **app user** and the connection is made by the **app user.** If the connection is established, activity data collected by the **Health App** will be provided to you for the purpose of providing additional, contextual information regarding the **app user's** activity. Please note that activity data is not validated by **myoncare tools** and should therefore not be used for diagnostic purposes as a basis for medical decision-making.

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

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

Purpose of processing activity data: App user´s activity data is provided to you for the purpose of providing additional, contextual information regarding the **app user's** activity. Please note that activity data is not validated by **myoncare tools** and should therefore not be used for diagnostic purposes as a basis for medical decision-making.

Justification of processing:
The data officer is the patient himself, by giving you access to his activity data for the purpose of reviewing the information shared. Therefore, no further justification is required.

PROCESSING OF PRODUCT SAFETY DATA

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

The **myoncare portal** and the **myoncare app** are classified and marketed as medical devices in accordance with European medical device regulations. As the manufacturer of the **myoncare tool**, we must comply with certain legal obligations (e.g. monitoring the functionality of the tool, evaluating incident reports that could be related to the use of the tool, tracking users, etc.). In addition, **myoncare tools** allow you to collect personal data about specific medical devices or medicines used in the treatment of your patients. The manufacturers of such medical devices or medicinal products also have legal obligations regarding market surveillance (e.g. collection and evaluation of side effect reports).
ONCARE is the data controller for the processing of product safety data.

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

Processing of product safety data: We store and evaluate all personal data in connection with our legal obligations as a manufacturer of a medical device and transmit this personal data (if possible after pseudonymization) to competent authorities, notified bodies or other data controllers with supervisory obligations. In addition, we will store and transfer personal data related to medical devices and/or medicines if we receive communications from you as the reporter of such information, from your 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 manufacturer of medical devices or medicinal products 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

Only applicable if you use myoncare tools for reimbursement.

The **myoncare portal** supports you in initiating your standard procedures for reimbursement for the healthcare services provided to your patients via the **myoncare app**. To enable the reimbursement process, the **myoncare portal** supports the collection of your patients' personal (health) data from the **myoncare**

portal in order to facilitate the transmission of this data to the patient's cost unit as part of the standard reimbursement processes (either your Association of Statutory Health Insurance Physicians and/or the patient's health insurance company). You are the data officer for the reimbursement data and responsible for compliance with data protection regulations for the processing of your patients' personal data in the reimbursement process. ONCARE acts as a data processor based on the data processing agreement with you as a **healthcare provider**.

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

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

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

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;
- 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 within one day;
(ii) if medication has been assigned;
(iii) if the **Privacy Policy** has been updated;
(iv) when an appointment is sent to patients and physicians, in particular 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
https://sendgrid.com/resource/general-data-protection-regulation-2/

Visible
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 operating system;
- User geolocation;
- Browser;
- Role;
- 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**.
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, please visit: https://matomo.org/privacy-policy/

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

We process and store personal data only for as long as 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 from and to the portal as well as from and to the app is encrypted. We offer SSL as an encryption protocol for secure data transmission. 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.

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

GENERAL INFORMATION ON CONSENT TO DATA PROCESSING

Your consent also constitutes consent to data processing under data protection law. Before granting us your consent, we will inform you about the purpose of the data processing and your right to object.
If the consent also relates to the processing of special categories of personal data, the **myoncare portal** will expressly inform you of this as part of the consent procedure.
Processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR may only take place if this is necessary due to legal provisions and there is no reason to assume that your legitimate interests preclude the processing of this personal data or that you have given your consent to the processing of this personal data in accordance with Art. 9 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 portal**. In addition, ONCARE will ask you to agree to a data processing agreement for the data processed by ONCARE under your responsibility as a data controller.

DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

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.

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 personal data. These service providers are Google (Google Firebase) cloud storage providers and support service providers.

Google Firebase is a "NoSQL database" that enables synchronization between the **myoncare portal** and your patient's **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 portal** and 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 service providers cannot establish a relationship with you as a data subject. This is achieved by encrypting the data during the transfer and using pseudo-keys to track these transfers instead of personal identifiers such as names or e-mail addresses. Re-identification takes place as soon as the personal data has reached the patient account in the **myoncare app** or in your account in the **myoncare portal** after verification 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 as well as that of your patient is stored. It also hosts myoncare's video and file management service, which enables encrypted video conferencing and data exchange between you and your patient. Access to your personal data by you and your patient is ensured by sending specific tokens. This personal data is encrypted during the transfer and pseudonymized for ONCARE and its service providers during the transfer and at rest. 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 recieving 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. This is a customer experience platform for dealing with 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

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.

Personal data collected by the **myoncare portal** or the **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.

Synchronization of the **myoncare portal** with the **myoncare app** takes place with the help of Google Firebase. Google Firebase servers are hosted in the European Union. Nevertheless, according to the general Google Firebase terms and conditions, a temporary data transfer to countries in which Google and related service providers have branches is 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. Unauthorized access to your data is prevented by end-to-end encryption and secure access tokens. Our online servers are hosted in Germany. For analysis purposes, the emails sent with SendGrid contain a so-called "tracking pixel" that connects to Sendgrid's servers when the email is opened. This can be used to determine whether an e-mail message has been opened.

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** use these interfaces, which are provided by Google, Apple and Withings, to request activity data from the connected health applications. 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 in particular to retention obligations under commercial or tax law.

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

YOUR RIGHTS AS A DATA SUBJECT

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 portal** and the various functions it offers.

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.

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 portal** from your computer. Please note, however, that we can only delete your personal data after the expiry of the statutory retention periods.

Right to rectification (Art. 16 GDPR): You can ask us to update or correct inaccurate personal data concerning you or to complete incomplete personal data.

Right to data portability (Art. 20 GDPR): In principle, you can request that we provide you with personal data that you have provided to us and that is processed automatically based on 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 based on your consent. We will continue to provide our services if they are not dependent on withdrawn consent.
To exercise these rights, please 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.

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

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

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

U.S. Privacy Policy PRIVACY POLICY

Welcome to myoncare, the digital health portal for efficient and needs-based patient care.
For us at Oncare GmbH (hereinafter referred to as "**ONCARE"** or "**we**", **"us**", "**our**"), the protection of your privacy and all personal data relating to you during the use of the myoncare portal is of great importance. We are aware of the responsibility that arises from the provision and storage of your personal data in the myoncare portal. 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 the applicable legal provisions on the protection of personal data. In this Privacy Policy, you will find out why and how ONCARE processes your personal data that we collect from you or that you provide to us when you decide to use the myoncare portal. In particular, you will find a description of the 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.

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.

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

In 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 (your patient).

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

"**Careplan Provider**" means you or any other service provider or third party (e.g. medical device manufacturer, pharmaceutical company) who makes Care Plans available to other Portal users via the myoncare Store or other means of data exchange.

"**Careplan User**" means you or any other service provider (Portal User) who uses a Care Plan ("Pathway") for the treatment of its registered Patients.

"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 themselves.

"**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 you or any other physician, clinic, healthcare facility or other healthcare professional acting alone or on behalf of you or another physician, clinic or healthcare facility (intended User).

"**Health Information**" means all information, including genetic information, whether recorded orally or in any form or on any medium, which
- is processed or transferred by a healthcare provider, health plan, health authority, employer, life insurer, school or university, or health clearing house; and

- relates to a person's past, present or future physical or mental health or a health condition also in connection with the person's medical treatment;
- 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**," "**HIPAA."** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that includes 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 App**" means the mobile myoncare application for use by patients who wish to use the services offered by Oncare.

"**myoncare Store**" is the platform operated by ONCARE that provides digital care concepts (care plans) for the treatment of your registered patients via the myoncare portal.

"**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 patients as **app users.**

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

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

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

"**Portal User**" means you or any other service provider using the web-based myoncare Portal.

ONCARE is a "business associate" as defined by HIPAA and provides services to both healthcare providers and health plans. These services are provided to entities designated as "covered entities" in HIPAA law; ONCARE concludes corresponding agreements with these institutions.
According to our Terms of Use, our offer is only aimed at patients aged 18 and over. Accordingly, no personal data of children and adolescents under the age of 18 is stored and processed.

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

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

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 and operates the interactive web portal **myoncare Portal** (for healthcare professionals) and the mobile application **myoncare App** (for patients) as access to the **myoncare services**. This **privacy policy** applies to all personal data processed by ONCARE in connection with the use of the **myoncare portal**. For the use of the **myoncare app** by patients, you will find a separate privacy policy for patients **here**.

ONCARE is a "business associate" (business associate in terms of **HIPAA**) that provides services and health plans to **healthcare providers**, which are referred to as "covered entities" within the meaning of HIPAA; ONCARE concludes business partner agreements with these covered companies. ONCARE will only use and

disclose **PHI** in accordance with the Business Associate Agreements and **HIPAA**.

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.

WHAT IS PERSONAL DATA IN TERMS OF THE GDPR

"**Personal data**" means any information that allows a natural person to be identified. In particular, this includes but is not limited to your name, birthday, address, telephone number, email address and IP address.

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

Data is to be considered "**anonymous**" if no personal connection to the person/user can be established. In contrast, "**pseudonymized**" data is data from which a personal reference or personally identifiable information is replaced by one or more artificial identifiers or pseudonyms, but which can generally be re-identified by the identifier key (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 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 provided to us when you register and log into our **myoncare portal,** contact us regarding problems with the portal or otherwise interact with us for the purpose of using the portal;

Treatment data: You collect personal data of your patients, such as name, age, height, weight, indication, symptoms of illness and other information in connection with the treatment of your patients in the **myoncare portal** (e.g. treatment data is personal data of your patients that is collected or processed when you contact your patient via the **myoncare portal** interact); Activity data of your connected patients will be made available to you in your **myoncare portal**.

Commercial Store Data: Personal data processed by us when you use the **myoncare store** either as an author of **careplan** or as a buyer of **careplan**. The use of the **myoncare store** requires the processing of your name and contact details as well as your payment data (payment data only if a **careplan** is subject to a fee).

Activity data: Personal data that is processed by us when an **app user** connects the **myoncare app** to a health app (e.g. AppleHealth, GoogleFit, Withings). Activity information of your affiliated patients is available to you within the **myoncare portal**.

Commercial and non-commercial research data: We process your personal data in anonymized/pseudonymized form in order to analyze and prepare summary scientific reports 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 as an incident reporter to meet legal security or vigilance purposes of medical device or pharmaceutical companies.

Reimbursement Data: Personal data required for the reimbursement process.

BLOCKCHAIN-TECHNOLOGY

Blockchain technology ("**Blockchain**") (European Patent No. 4 002 787) is an optional service that is not mandatory. It is up to you, the **healthcare provider**, to decide to use the blockchain solution. The **blockchain** is based on Hyperledger Fabric's technology. Hyperledger Fabric is 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 time, 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 determined that one copy has been modified, and the network deems that node to be faulty. This technical process prevents unauthorized people 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 in general, and to 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:

-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. 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.

In the event of patient synchronization, the integrity of the patient profile is also ensured by the blockchain. The **service 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 **service provider achieves sufficient** up-to-dateness regarding 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 based on Art. 28 GDPR (order processing agreement).

OPERATIONAL DATA PROCESSING

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

In the event of a service request, the following personal data can also be viewed by authorized ONCARE employees:
Your personal data that you have provided to us for registration and/or login to our portal (e.g. name, date of birth, profile picture, contact details).

Authorized ONCARE employees who may access your database for the purpose of processing a service request are contractually obligated to keep all personal information 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 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 that you are always informed about your tasks and important updates in order to optimally support your care.
- Emails are a reliable way to ensure that important information reaches you, even when push notifications are disabled.

Your options for action:

- If you do not want to receive push notifications, you can deactivate them in the settings of the **myoncare app.**
- Please ensure that your email address is accurate and up to date to ensure 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 processing operational data, ONCARE acts as a data officer responsible for the lawful processing of your personal data.

Types of Data: email address, date of birth, date of registration, your IP address, pseudo-keys generated by the Portal.

The app uses 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.

Purpose of processing operational data: We use the operational data to maintain the functionalities of the **myoncare portal** and to contact you directly if necessary or on your initiative (e.g. in the event of changes to terms of use, necessary support, technical problems, etc.). Furthermore, personal data (e-mail address) is required and processed within the framework of two-factor authentication every time you log in to the **myoncare portal**.

Justification of processing in accordance with the GDPR: The processing of personal data is justified based on 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 portal**.

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

PROCESSING OF TREATMENT DATA

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

- Adding a location;
- Uploading the logo of the site;
- Adding the details of the location;
- Uploading a Privacy Policy

It is possible to create further consent requirements for the patient, for which the patient must give consent in order to connect to the website.

An uploaded privacy policy will be displayed to every patient who connects to the website. All declarations of consent must be documented in the uploaded privacy policy. Once a privacy policy has been uploaded, it can only be replaced by a new version but cannot be deleted. The files are stored in a cloud database in Germany. You can allow the sharing of such files with other **portal users** within your institution for medical purposes. Other **portal users** do not have access to these files.

Furthermore, you may involve a **healthcare provider** outside your facility (consulting healthcare provider) in the treatment of your patients, provided you believe that an additional expert opinion would benefit the treatment.

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

We process such personal data, including the patient's health data, under an agreement with you and in accordance with your instructions.

GDPR rules

For the purpose of using the myoncare services with patients' health data, you are therefore the responsible data officer (in accordance with GDPR). Please only process your patients' data if you have obtained the required data consent from these patients. ONCARE will act as a processor (pursuant to GDPR) in accordance with the separate data processing agreement we agree upon with you based on Art. 28 GDPR.

PROCESSING OF COMMERCIAL STORE DATA

Only applicable if you use the myoncare store as a careplan user.

The **myoncare store** is integrated into the **myoncare portal** and offers the purchase of **care plans**. After registering with the **myoncare portal**, you can connect to the **myoncare store** using your login details. You can use the **myoncare Store** to purchase care plans as a user.

Data of the careplan user:

The data of the c**areplan user**, which the **myoncare store** processes during its use, is processed for the conclusion of a license agreement with the **careplan provider** – in this case ONCARE – and, if a fee is due, for the processing and control of the payment transaction between **the careplan provider** – in this case ONCARE – and **the careplan user**.

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

Processing commercial store data: Personal data that is processed by us in the case of using the myoncare store, either in the context of authorship of care plans or the purchase of care plans. In addition, the payment data (if a usage fee is charged) will be forwarded to the **careplan provider**.

GDPR rules

Justification for the processing of commercial store data: The legal basis for the processing of personal data is the separate order processing agreement that we concluded with the **careplan provider** based on Art. 28 GDPR.

PROCESSING OF ACTIVITY DATA

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

myoncare tools offer **app users** the option of connecting the **myoncare app** to certain health apps (e.g. AppleHealth, GoogleFit, Withings) ("**Health App**"), provided that these are used by the **app user** and the connection is made by the **app user.** If the connection is established, activity data collected by the **Health App** will be made available to you for the purpose of providing additional, contextual information regarding the **app user**'s activity. Please note that activity data is not validated by **myoncare tools** and should therefore not be used for diagnostic purposes as a basis for medical decision-making.

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

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

Purpose of Processing Activity Data: App User Activity Data is provided to you for the purpose of providing additional, contextual information regarding the **app user's** activity. Please note that activity data is not validated by **myoncare tools** and should therefore not be used for diagnostic purposes as a basis for medical decision-making.

Justification of processing:
The data officer is the patient themselves by giving you access to his activity data for the purpose of reviewing the information shared. Therefore, no further justification is required.

PROCESSING OF PRODUCT SAFETY DATA

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

The **myoncare portal** and the **myoncare app** are classified and marketed as medical devices in accordance with European medical device regulations. As the manufacturer of the **myoncare tool**, we must comply with certain legal obligations (e.g. monitoring the functionality of the tool, evaluating incident reports that could be related to the use of the tool, tracking users, etc.). In addition, **myoncare tools** allow you to collect personal data about specific medical devices or medicines used in the treatment of your patients. The manufacturers of such medical devices or medicinal products also have legal obligations regarding market surveillance (e.g. collection and evaluation of side effect reports).

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

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

Processing of product safety data: We store and evaluate all personal data in connection with our legal obligations as a manufacturer of a medical device and transmit this personal data (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 related to medical devices and/or medicines if we receive communications from you as the reporter of such information, from your 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

The legal basis for the processing of personal data for the fulfilment of legal obligations as a manufacturer of medical devices or medicinal products is Art. 6 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.

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 app;
- Create an account for the patient app;
- Patient application password reset workflow;
- 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 within one day;
(ii) if medication has been assigned;
(iii) if the Privacy Policy has been updated;
(iv) when an appointment is sent to patients and physicians, in particular for the "video call" appointment type;
(v) all information relating to a **Caretask** or if an **HCP** 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/

Visible

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, will your user behavior 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:
- Role;
- User geolocation;
- Browser;
- User operating system;
- 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 from and to the portal as well as from and to the app is encrypted. We offer SSL as an encryption protocol for secure data transmission. 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).

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.

Any transmission of personal data is encrypted during transmission.

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

GENERAL INFORMATION ON CONSENT

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.

GDPR rules

If the consent also relates to the processing of special categories of personal data, the **myoncare portal** will expressly inform you of this as part of the consent procedure. Processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR may only take place if this is necessary due to legal provisions and there is no reason to assume that your legitimate interests preclude the processing of this personal data or that you have given your consent to the processing of this personal data in accordance with Art. 9 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 portal.** In addition, ONCARE will ask you to agree to a data processing agreement for the data processed by ONCARE under your responsibility as a data controller.

DATA RECIPIENTS / CATEGORIES OF RECIPIENTS

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.

In certain cases, service providers support our specialist departments in the fulfilment of their tasks. The necessary data protection contracts have been concluded with all service providers who are processors (within the meaning of the GDPR) for health information / personal data. These service providers are Google (Google Firebase), cloud storage providers and support service providers.
Google Firebase is a "NoSQL database" that enables synchronization between the **myoncare portal** and your patient's **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 portal** and 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 service providers cannot establish a relationship with you as a data subject. This is achieved by encrypting the data during the transfer and using pseudo-keys to track these transfers instead of personal identifiers such as names or e-mail addresses. Re-identification takes place as soon as the personal data has reached the patient account in the **myoncare app** or in your account in the **myoncare portal** after verification 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 as well as that of your patient is stored. It also hosts myoncare's video and file management service, which enables encrypted video conferencing and data exchange between you and your patient. Access to your personal data by you and your patient is ensured by sending specific tokens. This personal data is encrypted during the transfer and pseudonymized for ONCARE and its

service providers during the transfer and at rest. 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

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 the **myoncare portal** or the **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 portal** with the **myoncare app** takes place with the help of Google Firebase. Google Firebase servers are hosted in the European Union. Nevertheless, according to the general Google Firebase terms and conditions, a temporary data transfer to countries in which Google and related service providers have branches is 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. Unauthorized 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 applications. 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 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.

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

SECURE TRANSFER 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 portal** and the various functions it offers.

AUTOMATED DECISIONS (IN ACCORDANCE WITH GDPR) IN INDIVIDUAL CASES

We do not use purely automated processing to make decisions.

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 of access (Art. 15 GDPR): You have the right to request information about whether and how your personal data is being processed, including information about the purposes of processing, recipients, storage period and your rights to rectification, 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 portal** from your computer. Please note, however, that we can only delete your personal data after the expiry of the statutory retention periods.

Right to rectification (Art. 16 GDPR): You can ask us to update or correct inaccurate personal data concerning you or to complete incomplete personal data.

Right to data portability (Art. 20 GDPR): In principle, you can request that we provide you with personal data that

you have provided to us and that is processed automatically on the basis of your consent or the performance of a contract with you in machine-readable form so that it can be "ported" to a substitute service provider.

Right to restriction of data processing (Art. 18 GDPR): You have the right to request the restriction of the processing of your personal data if the accuracy of the data is contested, the processing is unlawful, the data is needed 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 based on your consent. We will continue to provide our services if they are not dependent on withdrawn consent.

To exercise these rights, please 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.

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

DATA PROTECTION OFFICER (IN ACCORDANCE WITH GDPR)

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

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
* * * *