Privacy Notice for Patients

for the use of the myoncare mobile app and the myoncare Progressive Web App/PWA

Status March 2026

Introduction

The protection of your personal data, in particular your health data, is our highest priority. In this privacy notice, we transparently inform you about how personal data is processed when using the myoncare mobile app and the myoncare Progressive Web App/PWA (together referred to as myoncare “MOBILE”).

1. What is this privacy notice about?

This Privacy Notice explains how personal data are processed when you use the myoncare mobile app or the myoncare PWA as part of your care or services provided by a service provider (e.g., a medical practice, clinic, therapy facility, or other medical or non-medical providers of health, prevention, advisory, or care services). In particular, you will receive information about who is responsible for which processing activities, which data are affected, for what purposes the data are processed, and what rights you have.

2. Who is responsible for what? (Roles under the GDPR)

With myoncare, two entities are typically involved:

Your healthcare provider (e.g., your medical practice/clinic/medical facility): It decides on the purposes and means of processing your treatment and health data and is therefore the controller under data protection law (Art. 4(7) GDPR).

ONCARE GmbH (“ONCARE”): It provides the technical applications (mobile app/PWA) and, as a rule, processes treatment and health data exclusively on behalf of your healthcare provider as a processor (Art. 28 GDPR).
Important: The privacy notices shown to you during digital onboarding, as well as the collection of any required consents (e.g., for certain additional functions), are carried out exclusively in the name and under the responsibility of your healthcare provider. ONCARE has no influence on the content of your healthcare provider’s privacy notices or on whether and which consents are collected.

ONCARE does not make independent decisions about the purposes and means of processing treatment or health data. There is therefore no joint controllership within the meaning of Art. 26 GDPR in this respect.

In certain cases, ONCARE also processes data under its own responsibility, in particular where this is necessary for the secure technical operation of the app/platform (e.g., IT security, abuse prevention, provision of basic platform functions). In such cases, ONCARE is the controller within the meaning of the GDPR; its contact details are as follows:

3. Controllers and contact

3.1 Your healthcare provider (controller for treatment/health data)

The contact details of your healthcare provider (including data protection contact/data protection officer, if any) can be found in the privacy information provided by your healthcare provider (e.g., in the practice, on the website, or within onboarding).

3.2 ONCARE GmbH (processor and partially controller)

ONCARE GmbH
Postal address: Balanstraße 71a, 81541 Munich, Germany
E-mail: privacy@myoncare.com
Telephone: +49 (0) 89 4445 1156

3.2 Data Protection Officer of ONCARE

You can reach ONCARE’s Data Protection Officer at: privacy@myoncare.com

4. Principles of data processing, use of anonymized data

Medical personal data is not used for commercial or advertising purposes.
This does not affect if applicable the use of fully anonymized data where no personal reference exists anymore and re-identification is excluded according to the state of the art.
Such anonymized data is not subject to the GDPR and may if applicable be analyzed, combined, disclosed to third parties, or

sold by ONCARE for scientific, statistical, regulatory, quality assurance, and commercial purposes.
Such data does not contain any information that would allow conclusions to be drawn about individual persons.

5. What data is processed?

Depending on how the app/platform is used, the following data may be processed in particular—by category:

Master data and contact data (e.g., name, date of birth, address, health insurer, insurance number, e-mail address, phone number).
Account and usage data (e.g., login information, IP address, language settings, device information, log data).
Treatment and health data (special categories of personal data, Art. 9(1) GDPR), e.g., symptoms, photos, medication, questionnaire responses, diagnoses, therapies, treatment plans, progress and monitoring data, as well as completed/planned tasks.
Communication content (e.g., messages/approvals between you and the healthcare provider, insofar as the function is used).

6. For what purposes and on what legal basis is your data processed?

6.1 Provision of treatment via the app/platform (responsibility: healthcare provider)

Your healthcare provider uses myoncare to onboard you digitally, to carry out your medical treatment and care, and to communicate with you.

In doing so, your healthcare provider processes your personal data and—where necessary—health data, e.g., information on symptoms, diagnoses, therapies, medications, treatment plans, reminders, document/file exchange, questionnaires, monitoring. ONCARE processes this data on behalf of and under the instructions of the healthcare provider.

The legal bases are the responsibility of your healthcare provider. Typically applicable are:

- Art. 6(1)(b) GDPR (performance of the treatment contract or pre-contractual measures), and
- for health data Art. 9(2)(h) GDPR (healthcare/treatment) in conjunction with the applicable professional and statutory obligations.

Where consent is required for individual functions (e.g., optional additional services), your healthcare provider obtains and manages this consent. You can withdraw consent at any time with effect for the future; details can be found in your healthcare provider's information.

Where functions to support reimbursement or billing processes are used via the platform, your healthcare provider processes the data required for this under its own responsibility. ONCARE processes this data exclusively as a processor pursuant to Art. 28 GDPR.

6.2 Technical operation, IT security and abuse prevention (responsibility: ONCARE)

ONCARE processes certain data to ensure the secure technical operation of the app/platform, detect disruptions, and prevent unauthorized access.

This includes in particular:

- technical log data (e.g., times of access, device/browser information),
- security and access data (e.g., for authentication/password reset),
- an IP-based coarse geolocation to verify authorization to use and to detect unauthorized access (country/region only; no GPS data, no movement profiles).

The legal basis is Art. 6(1)(f) GDPR (legitimate interest in IT security and protection of particularly sensitive health data). Location data is used only selectively during the login process. Only the IP address and the coarse location information derived from it (e.g., country or region) are processed. No precise location data (e.g., GPS data), movement profiles, or permanent localization takes place. There is no merging of location data with other personal data and no profiling.

6.3 E-mail communication (responsibility: ONCARE or healthcare provider depending on content)

For certain functions (e.g., account creation, password reset, important system information, dispatch of reports), e-mails are sent. ONCARE uses e-mail service providers for this purpose. Content relating to your healthcare provider's medical communication is processed only under its instructions.

6.4 Product safety and vigilance data (medical device law)

To the extent the myoncare app/platform is operated as a medical device within the meaning of applicable European medical device regulations (e.g., Regulation (EU) 2017/745 – MDR), ONCARE is legally obliged to carry out market surveillance, product safety measures and to report serious incidents.

For this purpose, ONCARE may process personal data, including health data, to the extent necessary to fulfil these legal obligations.

The legal basis is
Art. 6(1)(c) GDPR (compliance with a legal obligation)
in conjunction with Art. 9(2)(i) GDPR (reasons of public interest in the area of public health).

Within this scope, ONCARE acts independently as the controller.

6.5 Activity and wearable data (optional)

If you voluntarily establish a connection to an external device or a health platform (e.g., wearable, fitness tracker, blood pressure monitor), activity or vital data may be transmitted to the platform.

This may include in particular:

- step counts
- sleep data
- heart rate
- blood pressure values
- other health parameters provided by the respective system.

Processing is carried out exclusively on the basis of your prior explicit consent pursuant to Art. 6(1)(a) GDPR and Art. 9(2)(a) GDPR.

Consent is voluntary and can be withdrawn at any time with effect for the future. ONCARE processes this data exclusively on behalf of the respective healthcare provider.

7. To whom is data disclosed?

Data is disclosed only if necessary (e.g., for operating the services), permitted by law, or if you/the healthcare provider have consented. Recipients may include in particular:

- Your healthcare provider and its authorized staff.
- ONCARE's technical service providers (sub-processors) for hosting, maintenance, support, e-mail dispatch—each contractually bound under Art. 28 GDPR.
- Service providers that process data under their own responsibility, e.g., Adobe when opening PDFs via an online service.

7.1.1 Hosting and cloud infrastructure

Depending on the customer, contractual setup, regulatory environment and country of use, ONCARE uses different hosting and cloud service providers. A logically separated system environment is operated for each healthcare provider. Personal data is stored in isolated server areas so that no commingling with data of other healthcare providers occurs.

Processing generally takes place within the EU/EEA. A transfer of personal data to countries outside the European Union or the European Economic Area takes place only if appropriate safeguards pursuant to Art. 44 et seq. GDPR exist (e.g., Data Privacy Framework (DPF) or EU Standard Contractual Clauses). Where necessary, supplementary safeguards are implemented.

7.1.2 Use of Cloudflare (Content Delivery Network and IT security)

For the secure and high-performance provision of the myoncare mobile app and the Progressive Web App (PWA), ONCARE uses the Cloudflare service.

Provider: Cloudflare Germany GmbH, Rosental 7, 80331 Munich, Germany
(parent company: Cloudflare Inc., USA).

Cloudflare is used as a so-called Content Delivery Network (CDN) and to protect against attacks (e.g., DDoS attacks). In doing so, the following technically required data may be processed in particular:

- IP address
- date and time of access

- content accessed
- browser and device information
- log data for attack detection

Processing is carried out exclusively for the purpose of:

- ensuring system security
- defending against cyberattacks
- ensuring availability
- optimizing loading speed and platform stability

The legal basis is Art. 6(1)(f) GDPR (legitimate interest in IT security and protection of particularly sensitive health data).

Cloudflare is used as a processor pursuant to Art. 28 GDPR. A corresponding data processing agreement exists.

Personal data may also be processed in the USA. Cloudflare is certified under the EU-U.S. Data Privacy Framework (DPF). In addition, appropriate safeguards pursuant to Art. 44 et seq. GDPR (in particular EU Standard Contractual Clauses) have been concluded.

The retention period for technically required log data is limited to the necessary minimum and is generally less than 24 hours unless a security-relevant evaluation is required.

Further information can be found at: https://www.cloudflare.com/privacypolicy.

The use of Cloudflare serves exclusively technical security purposes. Cloudflare does not perform any content analysis of medical data.

7.1.3 Use of Google Firebase

For technical synchronization between the myoncare app and your healthcare provider's platform, the Google Firebase service (Google Ireland Ltd., Dublin, Ireland) is used.

Only the data required for synchronization is processed. Processing is pseudonymized and encrypted. A direct assignment to your person is not possible for ONCARE and the technical service providers used.

Google is used as a processor pursuant to Art. 28 GDPR.

7.2 E-mail service providers (Brevo / SendGrid)

ONCARE uses Brevo (Sendinblue GmbH, Berlin) and SendGrid (Twilio Inc., USA) for the organizational sending of e-mails. Brevo or SendGrid may be used for transactional/confirmation e-mails. Data may be stored on the servers of the respective providers; with SendGrid, processing in the USA is possible. In these cases, appropriate safeguards pursuant to Art. 44 et seq. GDPR are used (e.g., EU Standard Contractual Clauses).

7.3 PDFs / online PDF display (Adobe)

If PDF documents are displayed within the app/platform via an Adobe online service, Adobe processes personal data under its own responsibility under data protection law. It cannot be ruled out that processing in the USA may also take place. Further information can be found in Adobe's privacy notice.

7.4 External links and social media content (e.g., Instagram)

The app/platform may contain links to external content (e.g., videos, podcasts, social media posts). By clicking on them, you leave the myoncare environment; the respective provider is responsible for data processing on the linked pages. When accessing such content, your browser may establish a direct connection to Instagram servers. Personal data (e.g., IP address, browser information) may be processed and cookies may be set, and transfers to third countries may occur. Individual services:

- Content from the Instagram service (Meta Platforms Ireland Ltd., Dublin, Ireland) may be displayed or linked. This may also occur if you do not have an Instagram account. If you are logged in to Instagram, the visit may be associated with your user account. Further information can be found in Instagram's privacy policy: https://privacycenter.instagram.com/policy/?entry_point=ig_help_center_data_policy_redirect

7.5 myon.clinic Store (optional)

If medical content or services are obtained or offered via the integrated myon.clinic Store, the content-related and commercial responsibility lies with myon.clinic GmbH (subsidiary of ONCARE GmbH). In this context, ONCARE provides only the technical platform. Contact: privacy@myon.clinic.

7.6 Support and ticketing systems

To handle technical service requests (e.g., password reset, changes to account data), ONCARE uses contractually bound support service providers. Only the account information necessary to process the request is processed.

Data processing agreements pursuant to Art. 28 GDPR exist with all support service providers. Staff are trained accordingly and bound to confidentiality.

7.7 Webfonts and display technologies

For a consistent and user-friendly display of the content of the myoncare mobile app and the Progressive Web App (PWA), fonts ("webfonts") may be used.

To the extent external services are used to provide fonts (e.g., Google Fonts), it may be technically necessary for your device to establish a connection to the provider's servers when accessing the platform. Technically necessary access data (e.g., IP address, browser type, device type, URL of the page accessed, date and time of access) may be processed.

Such processing is carried out exclusively for the functional display of the user interface and not for analysis, tracking, or marketing purposes.

To the extent personal data is transferred to countries outside the European Union or the European Economic Area, this takes place exclusively in compliance with the legal requirements of Art. 44 et seq. GDPR (e.g., on the basis of the Data Privacy Framework (DPF) or EU Standard Contractual Clauses).

7.8 Use of Matomo (optional usage analytics)

In order to improve the functionality and user friendliness of the myoncare Mobile App as well as the myoncare Progressive Web App PWA the analytics tool Matomo may be used. Matomo is an open source software used for the statistical evaluation of the use of the platform.

The analysis is carried out exclusively on servers under the control of ONCARE GmbH. No data is transmitted to external analytics providers.

The use of Matomo is disabled by default and will only be activated if the user expressly consents to the anonymized usage analysis.

If Matomo is activated technical usage information may be processed including in particular the operating system used the browser used the device type approximate geolocation such as country or region technical system information as well as interactions within the app or the PWA such as accessed functions or clicked buttons.

The IP address is shortened or anonymized prior to processing so that no direct personal reference can be established.

The processing is carried out exclusively for the purpose of better understanding the use of the platform improving functions and user friendliness and optimizing the technical stability and performance of the myoncare services.

If the user does not consent to the use of Matomo or withdraws such consent the user behavior will not be recorded.

The legal basis for the processing is Art. 6 para. 1 lit. a GDPR consent.

Further information is available at https://matomo.org/privacy-policy.

7.9 Optional use of AI based document recognition OCR

Within certain caretasks of the myoncare App users may optionally be offered the possibility to upload medical documents for example laboratory reports or findings in order to automatically extract the values contained therein.

This function is based on AI supported document recognition OCR Optical Character Recognition. For the technical processing an AI technology provided by Google LLC in particular Gemini may be used.

The use of this function is entirely voluntary. Users are expressly asked within the respective caretask whether they wish to use the automatic recognition. Alternatively all values can be entered manually at any time.

If a document is uploaded for automated analysis the following data may in particular be processed the uploaded document for example laboratory reports or findings the medical information contained therein for example laboratory values reference values or examination dates as well as technically required metadata for processing the document.

The processing is carried out exclusively for the purpose of automated extraction of the information contained in the document in order to facilitate the entry of medical values. The extracted data is subsequently displayed within the myoncare App and can be reviewed and confirmed by the user.

The AI used serves exclusively for technical text recognition and does not make any medical decisions.

The use of this function takes place exclusively on the basis of explicit consent. The legal basis is Art. 6 para. 1 lit. a GDPR consent as well as Art. 9 para. 2 lit. a GDPR consent to the processing of health data.

To the extent that personal data is processed by external technical services within the scope of this function a transfer to countries outside the European Union or the European Economic Area may take place. In such case the processing is carried out exclusively in compliance with the requirements of Art. 44 et seq. GDPR in particular on the basis of appropriate safeguards such as EU Standard Contractual Clauses or the EU US Data Privacy Framework.

The use of this function is voluntary and the use of the other functions of the myoncare App is also possible without using this OCR function.

8. How long is data stored?

ONCARE stores personal data only as long as necessary for the respective purposes and then deletes it, unless statutory retention periods prevent this. For treatment and health data, your healthcare provider's storage and retention obligations generally apply; you will receive information on this directly from your healthcare provider. Statutory retention and documentation obligations, in particular under medical device law, commercial law or tax law, remain unaffected.

9. Your rights

As a data subject, you have the rights set out in Art. 15 to 22 GDPR. These include in particular:

Right of access (Art. 15 GDPR)
You have the right to request information on whether personal data concerning you is being processed. If so, you have the right to information about the purposes of processing, categories of personal data, recipients, storage period and your further rights. You also have the right to a copy of the personal data.

Right to rectification (Art. 16 GDPR)
You can request the rectification of inaccurate personal data without undue delay or the completion of incomplete personal data.

Right to erasure (Art. 17 GDPR)
You can request the erasure of your personal data provided that the legal requirements are met. Please note that statutory retention and documentation obligations—especially in the medical field—may prevent erasure.

Right to restriction of processing (Art. 18 GDPR)
Under the statutory conditions, you can request restriction of processing.

Right to data portability (Art. 20 GDPR)
Where processing is based on your consent or a contract and is carried out by automated means, you have the right to receive the personal data you provided in a structured, commonly used and machine-readable format or to have it transmitted to another controller.

***Right to object (Art. 21 GDPR*)**
Where processing is based on Art. 6(1)(f) GDPR, you can object to processing on grounds relating to your particular situation.

Withdrawal of consent
Where processing is based on your consent, you can withdraw it at any time with effect for the future. The lawfulness of processing carried out up to the withdrawal remains unaffected.

Responsibility for exercising your rights

For the processing of your treatment and health data, your healthcare provider is the controller under data protection law. Please address related requests in principle to your healthcare provider.

ONCARE generally processes this data as a processor and supports the healthcare provider in fulfilling your rights within the framework of the data processing agreement.

Where ONCARE processes personal data under its own responsibility (e.g., for IT security or product safety purposes), you can exercise your rights at privacy@myoncare.com.

If your data is processed in the context of HIPAA-regulated treatment (see section 15), the competent Covered Entity or its Privacy Office is generally the point of contact for exercising your HIPAA rights.

Identity verification

To process your request, appropriate proof of identity may be required to ensure that personal data is not disclosed to unauthorized third parties.

Right to lodge a complaint

You also have the right to lodge a complaint with a data protection supervisory authority.

10. Withdrawal of consent

Where processing is based on your consent, you can withdraw it at any time with effect for the future. The lawfulness of processing up to the withdrawal remains unaffected. Please note: consents obtained by your healthcare provider (e.g., in onboarding) are generally managed via your healthcare provider.

11. Special case: use in corporate health management (BGM)

If you use the myoncare app as part of corporate health management (e.g., your employer), certain data may be shared with the company and, where applicable, commissioned data service providers in aggregated form, without being attributable to you as a person. In this scenario, the company (or a commissioned data provider) is typically the controller; ONCARE processes the data as a processor under their instructions. Details can be found in your company's BGM-specific information.

For managing support requests, the "RepairCode" tool (Digital Twin Code) may be used. This is a platform for structured processing of external requests. Further information can be found at: https://app.repaircode.de/?main=main-client - Rechtliches/privacy.

Where data is processed via a commissioned data service provider, this takes place exclusively on behalf of the respective controller.

12. Data security

ONCARE implements appropriate technical and organizational measures pursuant to Art. 32 GDPR to protect your data against unauthorized access, loss, alteration, or disclosure. This includes in particular:

- Encrypted data transmission (TLS)
- Encrypted storage of sensitive data
- Role- and authorization-based access concepts
- Logging of security-relevant access
- Hosting in secured data centers within the EU/EEA
- Regular security reviews
- Data storage only on servers with physical access control and ISO 27001 certification

For additional protection, personal identification features are replaced by pseudonymous keys in technical processes. Re-identification is possible only within your healthcare provider's secured system environment.
Access is only possible after successful authentication using secured token procedures.

13. Changes to this privacy notice

ONCARE may adapt this privacy notice, e.g., due to legal requirements or technical developments. Material changes will be communicated appropriately before taking effect (e.g., in the app/platform).

14. No automated decision-making

There is no solely automated decision-making within the meaning of Art. 22 GDPR. Medical decisions are made exclusively by your healthcare provider.

15. Additional notice for users in the USA (HIPAA)

If your health data is processed as part of treatment that is subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA), the HIPAA requirements apply in addition. HIPAA applies if a “Covered Entity” (e.g., a U.S. hospital/U.S. healthcare provider or a U.S. health insurer) is involved—regardless of the country in which you live.

In such cases, HIPAA information obligations (e.g., “Notice of Privacy Practices”) and HIPAA data subject rights are generally fulfilled by the respective Covered Entity.

Where the myoncare platform is used in a HIPAA context, the responsible U.S. group company myoncare Inc. acts as a “Business Associate” or “Sub-Business Associate” on the basis of a Business Associate Agreement (BAA). In these cases, ONCARE GmbH does not assume any responsibility under HIPAA.

For HIPAA requests (e.g., access in the form of a HIPAA “Access Request”), please contact the data protection office/Privacy Office of the treating Covered Entity; it will coordinate the processing, if necessary, with myoncare Inc.

Where both the GDPR and HIPAA apply, the respective obligations are fulfilled in a coordinated manner; responsibility for medical data processing remains with the treating entity.

***