PRIVACY POLICY

OncoCare.io Privacy Policy

Website, app, caregiver, provider, HIPAA-adjacent, and state-privacy disclosure framework.

Empowering patients. Supporting caregivers. Partnering with providers.

www.oncocare.io | info@oncocare.io | Last updated: April 20, 2026

HIPAA + State Privacy

OncoCare.io ("OncoCare," "we," "us," or "our") provides digital tools, education, and support for people affected by cancer and chronic illness, including patients, survivors, caregivers, and healthcare professionals. This Privacy Policy explains how OncoCare collects, uses, discloses, retains, and protects information through its websites, web and mobile applications, content, communications, and related services.

By accessing or using the Services, users agree to this Privacy Policy. If a user does not agree, the Services should not be used.

SCOPE

- The OncoCare.io website and related domains or subdomains.
- OncoCare Bloom and other OncoCare-branded digital products, portals, or applications.
- Email, SMS, in-app communications, events, webinars, surveys, and other interactions referencing this policy.
- This policy does not govern how healthcare providers, health plans, employers, or other third parties handle information under their own legal notices or privacy policies.

HIPAA ROLES

OncoCare.io may operate in more than one privacy role depending on the service model. In some contexts, OncoCare.io provides consumer-facing services directly to patients, survivors, or caregivers. In other contexts, OncoCare.io may provide technology or support services to a healthcare provider, health system, health plan, employer-sponsored program, or other regulated entity.

When OncoCare.io acts as a business associate for a HIPAA covered entity, it may receive, create, maintain, or transmit protected health information only as permitted by the applicable Business Associate Agreement and applicable law, and not for independent uses beyond what is authorized or legally allowed. [web:30][web:27][web:36]

When OncoCare.io collects data directly from individuals outside a HIPAA-governed relationship, that data may not constitute protected health information under HIPAA, but it may still be personal information or sensitive personal information under state privacy laws and is handled according to this policy. [web:22][web:30]

INFORMATION COLLECTED

Information provided directly

- Account, identity, and contact details, including name, email, phone, address, credentials, and profile details.
- Demographic details, such as age, date of birth, gender, ZIP code, and language preferences.
- Health and wellness information, including diagnosis, symptoms, side effects, medications, treatment activity, appointments, self-reported outcomes, mood, energy, nutrition, sleep, stress, journaling, and care-planning data.
- Information about caregivers, family, supporters, providers, and care-team members that users choose to add or share.
- Billing, subscription, support, survey, feedback, uploaded content, and communication records.

Information collected automatically

- Device, browser, operating system, IP address, app version, pages viewed, links clicked, timestamps, and approximate location.
- Analytics, usage, performance, and diagnostic information, such as session length, navigation patterns, crash data, and feature engagement.
- Cookies, pixels, SDKs, and similar technologies used for authentication, preference management, security, and platform improvement.
- Information received from providers, partners, benefit programs, integrations, and service providers where allowed.

USE OF INFORMATION

1. Operate, maintain, secure, and improve the Services.
2. Support care coordination, communication, symptom tracking, reminders, reporting, and user-directed sharing with caregivers or providers.
3. Personalize educational content, recommendations, and app experiences.
4. Respond to questions, support requests, operational notices, and service communications.
5. Support analytics, de-identified insights, product development, and lawful research activities.
6. Comply with legal obligations, investigate misuse, prevent fraud, and protect the rights, safety, and property of users and OncoCare.io.

SHARING OF INFORMATION

- With consent or at the user's direction, including sharing with caregivers, family, and providers selected by the user.
- With healthcare providers, health systems, health plans, or program sponsors when OncoCare.io is deployed as part of a clinical, care-management, navigation, or benefits program.
- With service providers supporting hosting, infrastructure, messaging, analytics, billing, security, and operations under contractual controls.
- For legal, compliance, safety, anti-fraud, incident response, or enforcement purposes when required or permitted by law.
- As part of a merger, acquisition, restructuring, financing, or asset sale, subject to lawful handling and continuity of protections.

- In aggregated or de-identified form for analytics, product development, and research purposes. [web:30][web:27]

CALIFORNIA PRIVACY RIGHTS

California residents may have rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, including the right to know what personal information is collected, used, disclosed, sold, or shared; the right to request deletion; the right to request correction of inaccurate information; the right to opt out of the sale or sharing of personal information where applicable; the right to limit the use and disclosure of sensitive personal information in certain circumstances; and the right not to be discriminated against for exercising privacy rights. [web:22][web:25][web:32]

OncoCare.io does not sell personal information for monetary consideration. If OncoCare.io engages in cross-context behavioral advertising or other activities that qualify as "sharing" under California law, California residents may exercise applicable opt-out rights and OncoCare.io will honor legally required preference signals such as Global Privacy Control where applicable. [web:22][web:29]

Requests may be submitted using the contact information below. OncoCare.io may need to verify identity before processing a request and may decline or limit a request where a lawful exception applies. [web:22][web:32]

OTHER STATE PRIVACY RIGHTS

Residents of certain other U.S. states may also have privacy rights, including rights to access, correct, delete, or obtain a copy of personal information, as well as rights to opt out of certain targeted advertising, sales, or profiling activities, depending on applicable law. OncoCare.io will process such requests in accordance with applicable state law and may require verification. [web:22][web:32]

SECURITY, BREACH RESPONSE, AND RETENTION

OncoCare.io uses administrative, technical, and physical safeguards designed to protect personal information, including encryption where appropriate, authentication controls, logging, monitoring, secure development practices, and vendor oversight. No environment can be guaranteed fully secure, but reasonable efforts are made to maintain appropriate safeguards. [web:30][web:31]

If a security incident or breach occurs, OncoCare.io will assess notification obligations under applicable federal and state law. Massachusetts requires reporting certain breaches affecting residents to state authorities, and breach notices are subject to state-specific rules. [web:31][web:28][web:34]

Information is retained for as long as reasonably necessary to deliver the Services, support contractual and clinical obligations, comply with law, resolve disputes, and enforce agreements. When information is no longer needed, it will be securely deleted or de-identified where feasible.

USER CHOICES

- Users may update certain account and profile information.
- Users may modify or remove certain logs or journal entries, subject to clinical or legal retention requirements.
- Users may opt out of marketing emails while still receiving essential service and account notices.
- Users may manage browser cookie settings and mobile-app permissions.
- Verified users may request access, correction, deletion, or additional privacy-rights review as available under applicable law. [web:22][web:32]

CHILDREN AND THIRD PARTIES

OncoCare.io is not directed to children under 13 without appropriate consent where required by law. In some cases, a parent, guardian, or provider may use the Services on behalf of a minor patient, and that adult is responsible for ensuring lawful authority and consent.

The Services may link to or integrate with third-party websites, tools, or applications. Their privacy practices are governed by their own notices and policies.

INTERNATIONAL USE AND POLICY CHANGES

Unless otherwise specified, OncoCare.io is intended primarily for users in the United States. Information may be processed in the United States or other jurisdictions where OncoCare.io or its service providers operate, subject to applicable safeguards where required.

This Privacy Policy may be updated from time to time. If material changes are made, the revision date will be updated and additional notice may be provided where required by law.

CONTACT

OncoCare.io
Email: info@oncocare.io
Website: www.oncocare.io
Mailing Address: 5 Cedar St, Unit 1, Roxbury, MA 02119