Murph Consumer Health Data Notice

Effective Date: April 29, 2026

Last Updated: April 29, 2026

Company: Just Cobuild, Co. ("Murph," "we," "us," or "our")

This Consumer Health Data Notice explains how Murph collects, uses, shares, and protects Consumer Health Data when you use Murph websites, hosted services, applications, integrations, onboarding flows, invite flows, messaging features, settings pages, APIs, and related services that link to this notice.

This notice supplements Murph's Privacy Policy. If this notice and the Privacy Policy conflict for Consumer Health Data, this notice controls to the extent required by applicable consumer health data privacy laws.

1. Scope

This notice applies to Murph-controlled processing of Consumer Health Data. It is intended to address U.S. state consumer health data privacy laws, including Washington's My Health My Data Act, Nevada's consumer health data privacy law, Connecticut consumer health data provisions, and similar laws that may apply to Murph.

This notice does not apply to:

- local or self-hosted Murph deployments, except where you send Consumer Health Data to Murph-controlled hosted services;
- information processed by third-party devices, wearable providers, identity providers, payment processors, messaging providers, model providers, search providers, or other integrations as independent providers under their own privacy policies;
- information exempt from applicable consumer health data privacy laws, such as protected health information under HIPAA where applicable, information governed by certain medical-record laws, or properly de-identified information; or
- employment or applicant information, unless a consumer health data law requires otherwise.

Murph is not a medical provider, hospital, pharmacy, emergency service, health plan, or medical device. Unless Murph expressly agrees otherwise in a separate signed writing, Murph is not acting as your HIPAA business associate and does not offer hosted Murph under a Business Associate Agreement.

2. What Consumer Health Data means

For purposes of this notice, Consumer Health Data generally means personal information that is linked or reasonably linkable to you and that identifies your past, present, or future physical or mental health status, condition, diagnosis, treatment, health-related behavior, or health-related service use.

Consumer Health Data may include information you provide directly, information imported from connected services, information generated by Murph, and information inferred from your use of Murph when that information identifies or is used to identify your physical or mental health status.

3. Categories of Consumer Health Data we may collect

Depending on the features you use and the choices you make, Murph may collect:

- Health, wellness, and lifestyle records, such as symptoms, observations, routines, habits, meals, foods, recipes, supplements, protocols, goals, health history, medications you choose to log, and other wellness notes.
- Wearable, device, and activity data, such as sleep, recovery, readiness, activity, heart rate, heart-rate variability, temperature, respiration, blood oxygen, movement, workout, body-state, or similar measurements from connected services or devices.
- User-generated content, such as journals, prompts, messages, conversations, assistant requests, files, attachments, photos, audio, transcripts, parsed content, and metadata that may identify or describe your health status.
- Derived, inferred, and generated information, such as trends, summaries, classifications, recommendations, reminders, before-and-after analyses, experiment results, protocol outputs, and other outputs generated from your data.
- Connected-service and integration information, such as connection status, authorization metadata, provider account identifiers or privacy-preserving lookup values, sync timestamps, webhook traces, reconciliation records, error metadata, and routing information needed to operate an integration.
- Invite, import, export, and collaboration information, such as invite codes, recipient lookup values, preview metadata, acceptance status, imported record bundles, exported records, and records of whether an invite or imported item was accepted, rejected, expired, or consumed.
- Account, contact, support, and communications information associated with Consumer Health Data, such as your name, alias, email address, phone number, account identifiers, authentication status, support messages, privacy requests, and operational records when they relate to your use of health-related Murph features.
- Technical and usage information associated with Consumer Health Data, such as IP address, device and browser information, timestamps, request identifiers, session information, crash logs, diagnostic logs, and security events when needed to provide, secure, debug, or support health-related features.

Murph does not intentionally collect precise geolocation information for the purpose of identifying visits to health care facilities or targeting health-related messages. If you choose to include location information in your content or connected data, Murph may process that information as part of the feature you requested.

4. Sources of Consumer Health Data

Murph may collect Consumer Health Data from:

- you, when you create an account, complete onboarding, send a prompt or message, log a meal, routine, symptom, supplement, protocol, note, or observation, upload a file, contact support, or submit a privacy request;
- your devices, browsers, and Murph deployments, when you use Murph or connect local and hosted workflows;
- connected providers and integrations you authorize, such as wearable, activity, communication, identity, storage, or data-source providers;
- other Murph users or invite participants, when they send you an invite, share information with you, or include your information in a Murph flow;
- service providers and processors, such as hosting, security, authentication, logging, messaging, billing, support, model, search, parsing, analytics, or diagnostics providers that help Murph operate; and

- information generated by Murph, such as summaries, trends, classifications, reminders, analyses, and other outputs created from your Consumer Health Data.

5. Purposes for collecting, using, and processing Consumer Health Data

Murph may collect, use, and process Consumer Health Data to:

- provide Murph and the features you request;
- create and manage accounts, sessions, settings, permissions, subscriptions, and support workflows;
- sync, import, display, search, organize, analyze, summarize, export, or share records at your direction;
- operate connected-service, wearable, device, messaging, invite, import, export, and automation features;
- generate assistant responses, reminders, insights, experiment results, before-and-after analyses, protocol outputs, and other requested outputs;
- process prompts, messages, attachments, files, transcripts, and related context;
- communicate with you about service, security, support, onboarding, billing, account, legal, and privacy matters;
- secure Murph, prevent misuse, detect fraud or abuse, debug issues, monitor reliability, maintain audit records, and protect users and the service;
- comply with law, respond to legal process, enforce agreements, protect rights, and handle disputes;
- process transactions, subscriptions, renewals, refunds, invoices, taxes, and accounting records;
- maintain, test, develop, and improve Murph using aggregated, de-identified, pseudonymized, or otherwise minimized information where feasible; and
- handle other purposes disclosed to you with any consent required by law.

Murph does not use Consumer Health Data you submit through Murph to train, fine-tune, or improve Murph's or any third party's general-purpose AI models. This commitment applies even if you provide feedback. Separate research consents, if offered, will be limited to the research or product-evaluation purpose described in that consent and will not authorize general-purpose AI model training on Consumer Health Data. We also require third-party AI model providers that process Consumer Health Data for the Hosted Service not to use that data to train their models.

6. Categories of Consumer Health Data we may share

Murph may share the categories of Consumer Health Data listed in Section 3 when sharing is necessary for the purposes described in Section 5, when you direct us to share it, when required or permitted by law, or when you provide consent.

For example, Murph may share:

- account, contact, authentication, and settings information needed to operate hosted Murph;
- health, wellness, wearable, device, activity, user-generated, derived, inferred, generated, invite, import, export, and collaboration information needed to provide requested features;
- prompts, messages, attachments, files, transcripts, and related context needed to provide assistant, search, parsing, extraction, summarization, or automation features;
- integration metadata and routing information needed to operate connected services;
- technical, diagnostic, logging, security, and support information needed to operate, debug, secure, and support Murph; and

- transaction, billing, subscription, and entitlement information needed to process payments and manage account status.

7. Categories of recipients

Murph may share Consumer Health Data with:

- service providers and processors that help Murph provide, host, store, secure, debug, monitor, analyze, support, or improve the service;
- identity, authentication, and account providers that help verify users, manage sessions, and operate sign-in flows;
- cloud hosting, infrastructure, database, storage, and deployment providers that help operate hosted Murph;
- messaging, email, phone, notification, and communication providers that help deliver service, support, authentication, invite, or user-directed messages;
- payment and billing processors that help process subscriptions, invoices, receipts, refunds, disputes, fraud checks, taxes, and account entitlements;
- model, search, parsing, extraction, transcription, automation, and assistant providers that help power features you request;
- analytics, diagnostics, logging, monitoring, security, and abuse-prevention providers that help operate, secure, and improve Murph;
- connected services and integrations you enable;
- people or organizations you direct Murph to share with, such as recipients of invites, exports, collaboration flows, or messages;
- professional advisers and legal, compliance, and safety recipients where disclosure is required or permitted by law or needed to protect rights, safety, privacy, or property; and
- successors or transaction participants, subject to appropriate legal and confidentiality protections.

Murph does not currently share Consumer Health Data with any corporate affiliate. If that changes, Murph will update this notice and obtain any consent required by law before sharing Consumer Health Data with that affiliate.

Murph requires processors to process Consumer Health Data only according to Murph’s instructions, use appropriate safeguards, assist with consumer-rights requests where required, and process Consumer Health Data consistently with this notice and applicable law.

8. Sale, advertising, and tracking

Murph does not sell Consumer Health Data.

Murph does not use Consumer Health Data for targeted advertising, cross-context behavioral advertising, retargeting, lookalike audiences, ad attribution, ad measurement, or health-data advertising profiles.

Murph does not knowingly permit third parties to collect Consumer Health Data over time and across different websites or online services through Murph for targeted advertising or data-sale purposes. Some service providers may collect technical, usage, diagnostic, security, or communications information through Murph as needed to provide services to Murph or to you.

If Murph ever seeks to sell Consumer Health Data, Murph will not do so unless it first provides the disclosures and obtains the separate written authorization required by applicable law. Murph will not condition goods or services on signing an authorization to sell Consumer Health Data where prohibited by law.

9. Your Consumer Health Data rights

Subject to applicable law and verification, you may have the right to:

- confirm whether Murph is collecting, using, sharing, or selling Consumer Health Data about you;
- access Consumer Health Data about you;
- receive information about the categories of Consumer Health Data Murph collects, uses, shares, or sells;
- receive a list of categories of third parties and affiliates with whom Murph has shared Consumer Health Data and, where required by law, a list of specific third parties or affiliates and a way to contact them;
- review and request changes or corrections to Consumer Health Data about you;
- withdraw consent for future collection or sharing of Consumer Health Data where Murph relies on consent;
- request that Murph cease collecting, sharing, or selling Consumer Health Data about you where applicable law provides that right;
- request deletion of Consumer Health Data about you;
- appeal Murph’s refusal to act on a Consumer Health Data request where applicable law provides an appeal right; and
- be free from unlawful discrimination for exercising Consumer Health Data rights.

These rights may be limited by exceptions under applicable law, including legal obligations, security needs, fraud prevention, dispute handling, free-speech rights, the rights of others, or our ability to verify your identity and authority.

10. How to exercise rights, withdraw consent, or appeal

To exercise Consumer Health Data rights, contact Murph at legal@justco.build. Please use the subject line "Consumer Health Data Request" and describe the right you want to exercise.

Murph may need to authenticate your identity and authority before acting on a request. You do not need to create a new Murph account to submit a request, but if you already have a Murph account, Murph may require you to use that account or otherwise verify control over the relevant email address, phone number, account, device, integration, or other identifier.

Where permitted by law, you may use an authorized agent to submit a request. Murph may require proof that the agent is authorized to act for you and may ask you to verify your identity directly.

For Consumer Health Data requests covered by applicable law, Murph will respond within the time required by law, including within 45 days where Washington law requires it. When allowed by law, Murph may use one 45-day extension if reasonably necessary and will tell you why.

Where Murph relies on your consent to collect or share Consumer Health Data, you may withdraw consent for future processing by contacting legal@justco.build or by using available product controls, such as disconnecting an integration, changing settings, revoking a provider authorization, deleting an invite, or closing your account.

Withdrawal of consent does not affect processing that occurred before withdrawal. Some Murph features may stop working or become unavailable if you withdraw consent, disconnect an integration, or ask Murph to stop collecting or sharing Consumer Health Data needed to provide a requested feature.

If Murph denies your Consumer Health Data request and applicable law gives you an appeal right, you may appeal by replying to Murph's decision or by emailing legal@justco.build with the subject line "Consumer Health Data Appeal."

Murph will review the appeal and respond within the time required by applicable law, including within 45 days where Washington law requires it. If Murph denies the appeal where consumer health privacy law requires regulator-contact information, Murph will explain the reason for the denial and provide the applicable complaint mechanism or other method for contacting the relevant regulator or attorney general.

11. Deletion

You may request deletion of Consumer Health Data about you by contacting legal@justco.build with the subject line "Consumer Health Data Deletion Request."

After Murph verifies your request, Murph will delete Consumer Health Data covered by the request from Murph's records and notify affiliates, processors, contractors, and other third parties with whom Murph has shared that Consumer Health Data, as required by applicable law.

Deletion may be limited or delayed where permitted by law, including for legal compliance, security, fraud prevention, dispute handling, exercise or defense of legal claims, protection of other users, or backup and archival systems. If applicable law permits delayed deletion from backup or archival systems, Murph will limit further processing of that data until deletion is completed unless another legal basis permits processing.

12. Security

Murph uses administrative, technical, and physical safeguards designed to protect Consumer Health Data. These safeguards may include encryption in transit, encryption at rest for certain hosted data, access controls, least-privilege practices, privacy-preserving identifiers or lookup values, logging, monitoring, abuse-prevention controls, secure key handling, signed internal requests, vendor management, and staff access limits.

No method of transmission or storage is completely secure. Hosted Murph is not a zero-knowledge, operator-blind, or end-to-end-encrypted service unless Murph expressly says otherwise for a specific feature.

13. Changes to this notice

Murph may update this notice from time to time. When Murph does, it will revise the "Last Updated" date above and provide any additional notice required by law.

Murph will not collect, use, or share additional categories of Consumer Health Data, use Consumer Health Data for additional purposes, or share Consumer Health Data with additional categories of third parties or affiliates in ways that require consent under applicable law unless Murph first updates its disclosures and obtains any consent required by law.

14. Contact

For questions, requests, appeals, complaints, or withdrawal of consent related to Consumer Health Data, contact:

Murph Privacy Team

Email: legal@justco.build