Murph Privacy Policy

Effective Date: April 9, 2026 Last Updated: April 29, 2026

Murph ("Murph," "we," "us," or "our") provides software and services designed to help people understand their bodies and lives better through tools such as health journaling, meal tracking, wearable and device sync, messaging-based interactions, hosted onboarding, invite, import, export, and related local or hosted experiences.

This Privacy Policy explains how we collect, use, disclose, and otherwise process information when you:

- use Murph's websites, applications, hosted services, local or self-hosted deployments, and related operator tools;
- create or use a Murph account;
- connect third-party services, devices, or communication channels to Murph;
- interact with Murph through email, messaging, passkey, phone verification, or other supported interfaces; or
- otherwise communicate with us about Murph.

This Privacy Policy does not govern third-party services, devices, identity providers, payment providers, model providers, search providers, messaging providers, wearable providers, or other integrations except to the extent Murph acts as the controller for information we receive from or send to them in connection with Murph. Those third parties may have their own privacy policies and terms.

1. Scope and deployment model

Murph may be used in more than one way:

1. Local or self-hosted use. If you run Murph on your own device, workstation, or infrastructure, more of your data may remain within systems you control. In that case, your own infrastructure, configuration choices, and selected providers may determine much of the privacy and security posture.
2. Hosted Murph services. If you use Murph's hosted onboarding, billing, messaging, invite, import, export, wearable sync, email sync, device sync, or execution features, Murph and its service providers may process information needed to provide and support those features.

This Privacy Policy applies to Murph-controlled processing. If you self-host Murph or connect Murph to providers of your choosing, your use of those providers and systems may also be subject to separate privacy policies, terms, security settings, and retention practices that Murph does not control.

2. Our privacy commitments

Murph is designed for sensitive personal and health-related information. We make the following commitments:

- No sale or rental. We do not sell or rent personal information.
- No sale, sharing, licensing, or data-broker disclosure of health data. We do not sell, rent, license, disclose, or make available health data, consumer health data, HealthKit data, wearable data, journal content, health files, health memories, prompts involving health data, or derived health insights to data brokers, advertising networks, third-party advertising platforms, information resellers, or similar parties.

- No targeted advertising from health data. We do not use health data for cross-context behavioral advertising, targeted advertising, retargeting, lookalike audiences, ad attribution, ad measurement, or health-data advertising profiles.
- No health data for insurance, employment, credit, or eligibility decisions. We do not disclose health data to employers, insurers, lenders, benefits administrators, or credit agencies for eligibility, underwriting, pricing, employment, benefits, credit, or risk-scoring decisions, unless you expressly direct us to do so for a specific feature and applicable law permits it.
- No AI training on health data. We do not use health data, consumer health data, HealthKit data, wearable data, journal content, health files, health memories, health prompts, assistant outputs based on health data, or derived health insights to train, fine-tune, or improve Murph's or any third party's general-purpose AI models.
- Limited provider use. When we use service providers, subprocessors, model providers, search providers, wearable connectors, health-record connectors, or infrastructure providers, we authorize them to process information only as needed to provide, secure, support, or troubleshoot Murph, subject to contractual and legal safeguards where applicable.
- Feature-specific consent for optional health integrations. We collect health data from optional integrations only when you enable the integration or otherwise provide affirmative, feature-specific consent. You can withdraw consent by disconnecting the integration or contacting us.
- Need-to-know access. We limit access to personal information and hosted health data to authorized personnel and service providers who need it to operate, secure, support, or troubleshoot Murph. We use aggregated or de-identified information for service improvement as described below.
- No hidden ad-tech on health surfaces. We do not intentionally place third-party advertising pixels, retargeting tags, behavioral advertising SDKs, or similar technologies on pages, screens, APIs, or workflows where users enter, view, upload, connect, or receive health data.
- Transparent hosted processing. Unless we expressly state otherwise for a specific feature, Hosted Murph is not zero-knowledge, operator-blind, or end-to-end encrypted. Hosted Murph may require Murph and its providers to process readable content to provide requested features, support users, debug problems, secure the service, or comply with law.
- HIPAA boundary. Unless we enter into a written Business Associate Agreement that expressly covers the relevant service, Murph is not acting as a HIPAA business associate and Hosted Murph is not offered under a BAA.
- Local control. If you run Murph locally or self-host Murph, Murph does not receive your local health content unless you connect hosted Murph services, enable telemetry, use a hosted integration, request support, or otherwise transmit information to us.

3. Information we collect

We may collect the following categories of information, depending on how you use Murph.

A. Account, identity, and contact information

This may include:

- name, display name, username, or alias;
- email address and/or phone number;
- account identifiers, authentication identifiers, passkey-related identifiers, linked-wallet identifiers, session information, or linked-account identifiers;
- invite, verification, or onboarding status information; and

- support communications and account preferences.

B. Health, wellness, and user-provided content

Murph is built around information you choose to provide, generate, connect, or import, including:

- journals, notes, observations, symptoms, routines, meals, foods, recipes, supplements, protocols, and related wellness records;
- wearable, device, activity, sleep, recovery, or body-state information from connected providers or devices;
- heart rate, movement, temperature, respiration, blood oxygen, readiness, recovery, activity, or similar measured or derived data, where available through connected services or your own inputs;
- prompts, questions, conversations, messages, and other content you send to Murph;
- files, attachments, photos, audio, transcripts, parsed content, and related metadata; and
- information included in invite flows or imported record bundles.

Some of this information may constitute health data, sensitive personal information, special category data, or consumer health data under applicable law.

C. Connected-service and integration data

If you connect devices, accounts, or communication channels, we may collect:

- connection and authorization metadata;
- provider account identifiers or privacy-preserving lookup values;
- token or credential-related metadata;
- connection status, sync timestamps, webhook traces, and reconciliation or error metadata; and
- minimal routing or message metadata needed to operate the integration.

D. Communications, support, and assistant data

We may collect:

- support requests, feedback, bug reports, and troubleshooting details;
- inbound or outbound email, message, or other channel metadata necessary to provide the service;
- prompts, chat history, tool inputs, tool outputs, and related context needed to provide assistant, search, or automation features; and
- records of how privacy, support, or account requests were handled.

E. Invite and collaboration data

If you use Murph invite or collaboration features, we may collect:

- invite codes and invite metadata;
- recipient contact details or lookup values;
- preview metadata, acceptance status, and consumption or expiry data; and
- records of whether and when an invite or imported item was accepted, rejected, expired, or consumed.

F. Billing and transaction information

If you purchase, subscribe to, or otherwise pay for hosted Murph features, we and our payment processors may collect:

- billing contact information;

- subscription, entitlement, or account-status information;
- checkout, invoice, transaction, or payment-status metadata;
- customer, subscription, checkout-session, or similar processor-issued identifiers; and
- fraud-prevention or payment-authentication information.

Murph does not need to store full payment card numbers to provide ordinary hosted billing functionality. Payment card details are typically processed by our payment processor.

G. Technical, device, and usage information

We may collect information such as:

- IP address;
- browser, device, app, operating-system, and version information;
- timestamps, request identifiers, crash or error logs, and performance metrics;
- cookie, local-storage, or session-token data used to operate core features; and
- security, abuse-prevention, and diagnostic information.

4. Sources of information

We collect information from several sources:

- Directly from you, when you create an account, complete onboarding, use a feature, upload content, send a prompt or message, or contact us.
- From your devices and browsers, when you use Murph.
- From connected providers or integrations, when you choose to link them to Murph.
- From identity and authentication providers, when you sign in, verify an account, or complete an onboarding flow through them.
- From payment processors, when you purchase or subscribe to hosted services.
- From other Murph users, such as when someone sends you an invite link.
- From service providers and security tools, where needed to operate, support, analyze, or secure Murph.

5. How we use information

We may use information for the following purposes.

A. To provide Murph and requested features

We use information to:

- create and manage accounts and sessions;
- authenticate users and verify access;
- sync, display, search, organize, and export records;
- operate wearable and provider connections;
- process prompts, messages, attachments, and requested outputs;
- deliver hosted onboarding, invite, import, and export flows;
- enable billing, entitlement, and subscription management; and
- provide customer support and respond to requests.

B. To operate, maintain, and improve Murph

We use information to:

- monitor reliability, availability, security, and performance;
- debug and repair errors;
- understand feature usage at a service level;
- improve Murph's features, workflows, and user experience; and
- test, develop, and support new capabilities.

Where feasible, Murph prefers to use aggregated, de-identified, pseudonymized, or otherwise minimized data for product and service improvement.

For health data and consumer health data, Murph uses identifiable data for product improvement only where necessary to provide, secure, support, troubleshoot, or maintain features you use; where you have provided any required consent; or where the data has been aggregated, de-identified, pseudonymized, or otherwise minimized as described in this Policy. Product improvement does not include targeted advertising, data brokerage, insurance/employment/credit eligibility decisions, or general-purpose AI model training.

C. To secure Murph and prevent misuse

We use information to:

- detect, investigate, and prevent fraud, abuse, spam, or unauthorized access;
- enforce our Terms and policies;
- maintain logs, audit trails, and security controls;
- protect Murph, our users, and third parties; and
- respond to incidents and preserve evidence where appropriate.

D. To process transactions and administer commercial relationships

We use information to:

- process payments, subscriptions, renewals, and refunds;
- manage billing records, receipts, disputes, and account status; and
- comply with accounting, tax, and recordkeeping obligations.

E. To communicate with you

We use information to:

- send service, security, support, onboarding, and billing communications;
- deliver transactional messages you request or enable;
- respond to questions, feedback, and privacy requests; and
- send legally permitted updates or, where applicable, marketing communications with opt-out choices.

F. To comply with law and protect rights

We may use information to:

- comply with legal obligations and regulatory requirements;
- respond to lawful requests and legal process;
- establish, exercise, or defend legal claims; and
- protect the rights, safety, privacy, or property of Murph, our users, or others.

6. Health data, AI, and model providers

Murph may use AI, search, parsing, transcription, embedding, summarization, extraction, retrieval, and automation features to provide the functionality you request. These features may process prompts, messages, health records, journal entries, wearable data, files, attachments, transcripts, health memories, and related context.

Murph tries to limit the data shared with those systems or providers to what is reasonably necessary for the requested feature. Where feasible, Murph may minimize, pseudonymize, redact, hash, or otherwise reduce the data used.

No model training on health data. Murph does not use health data, consumer health data, HealthKit data, wearable data, journal content, health files, health memories, prompts involving health data, assistant outputs based on health data, or derived health insights 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 health data.

Third-party model providers. Murph does not route health data to third-party model, search, parsing, transcription, embedding, or inference providers unless the relevant contract, service setting, or deployment control prohibits model training on Murph health data. We also require those providers to limit retention of Murph health data to what is necessary to provide, secure, and troubleshoot the requested service.

Health memories and derived context. If Murph creates persistent health memories, summaries, embeddings, trends, user preferences, or other derived context from your health data, we treat those derived items as health data. Health memories are used only to provide, personalize, secure, support, or troubleshoot Murph features you use. You may request access, correction, deletion, or disabling of health memories where required by law and supported by the feature.

Human review. Murph personnel do not review the contents of your hosted health data except where needed to provide support you request, investigate security or abuse issues, debug service problems, comply with law, enforce our Terms, or protect the rights, safety, privacy, or property of Murph, users, or others.

Important outputs disclaimer. AI-generated outputs may be incomplete, inaccurate, or inappropriate for your situation. Murph is designed for personal wellness, journaling, organization, education, and self-reflection. Murph is not a medical device, does not provide medical diagnosis or treatment, and is not a substitute for professional medical advice or emergency care.

7. Legal bases for processing

If you are in the EEA, UK, Switzerland, or another jurisdiction that requires a legal basis for processing, Murph may process personal data on one or more of the following bases:

- Performance of a contract: to provide Murph and the features you request.
- Legitimate interests: to secure, maintain, support, and improve Murph, provided those interests are not overridden by your rights.
- Consent: where required, including for certain sensitive-data processing, optional integrations, optional permissions, or specific marketing activities.
- Legal obligation: where processing is required to comply with applicable law.
- Vital interests or other lawful bases, where applicable.

Where Murph relies on consent, you may withdraw it for future processing at any time, subject to legal and operational limits. Withdrawing consent may limit your ability to use certain features.

8. How we disclose information

We may disclose information in the following circumstances.

A. Service providers and processors

We may share information with vendors, service providers, and subprocessors that help us operate Murph, such as providers for:

- identity and authentication;
- cloud hosting, storage, and infrastructure;
- messaging, email, and communications;
- payments and billing;
- customer support, logging, monitoring, and security;
- search, model, parsing, or other optional feature providers; and
- analytics or diagnostics used to operate and improve Murph.

These parties are authorized to process information on Murph's behalf only as needed to provide services to us or to you, subject to contractual and legal safeguards where applicable.

Subprocessors and model providers. We maintain a list of subprocessors and third-party providers that may process personal information or health data for Murph at withmurph.ai/subprocessors (https://withmurph.ai/subprocessors). The list identifies the provider or provider category, service purpose, categories of data involved, country or region, and whether the provider is permitted to use Murph data for training. Material changes to Murph-managed providers that process health data will be reflected on that page and, where required by law or contract, notified to users.

B. Connected services and integrations you enable

If you connect Murph to devices, wearable providers, messaging channels, identity providers, or other third-party services, Murph may exchange information with those services as needed to provide the feature you requested.

Feature-specific consent. We collect, use, or disclose health data from optional integrations only after you enable the integration or otherwise provide affirmative, feature-specific consent. Consent screens will describe the data source, categories of data requested, purpose of use, whether data will be stored or queried on demand, the categories of recipients or named providers involved, and how you can withdraw consent. Where applicable law requires separate consent for collection and sharing, Murph will request those consents separately. You can withdraw consent by disconnecting the integration or contacting us. Withdrawal stops future collection from that integration, but may not affect data already processed as permitted by law, data retained for security or legal reasons, or data already extracted by an independent third party you directed us to share with.

When you direct Murph to share information with a third-party provider, that provider may act as an independent controller of the information it receives under its own privacy policy and terms. Please review those policies carefully before enabling a connection.

C. Invites and user-directed disclosures

If you create, send, or accept a Murph invite or similar user-directed flow, Murph may disclose the information reasonably necessary to complete that flow to the intended recipient or the service providers involved in carrying it out. Depending on the feature, this may include preview information, invite status, or imported records.

Information you intentionally make available to other users or recipients may become visible to them under the settings or permissions you choose.

Recipient responsibility. If you direct Murph to share health data with another person, organization, workspace, coach, clinician, researcher, or third-party app, that recipient may become an independent controller or separately responsible party for the data it receives. Their privacy policy, security practices, retention periods, and deletion practices may apply. Murph is not responsible for data that a recipient independently extracts, stores, or further discloses outside Murph, except where applicable law says otherwise.

D. Legal, compliance, and protection purposes

We may disclose information if we believe doing so is reasonably necessary to:

- comply with law, regulation, legal process, or lawful governmental request;
- enforce our agreements or policies;
- detect, prevent, or address fraud, security, or technical issues; or
- protect the rights, privacy, safety, or property of Murph, our users, or others.

Government and law-enforcement requests. Murph does not voluntarily disclose health data to law enforcement, government agencies, or civil litigants except with your direction, as required by valid legal process, or where we reasonably believe disclosure is necessary to prevent serious harm, protect rights or safety, or comply with law. Where legally permitted and reasonably practicable, we will attempt to notify you before disclosing your information in response to legal process. We may challenge requests that we believe are overbroad, unlawful, or inconsistent with user privacy.

E. Corporate transactions

If Murph is involved in a merger, acquisition, financing, reorganization, bankruptcy, sale of assets, or similar transaction, personal information may be disclosed or transferred subject to appropriate confidentiality, security, and legal protections. Consumer health data will not be transferred for materially different uses unless the recipient is bound to protections materially consistent with this Privacy Policy, we provide notice required by law, and we obtain any consent or authorization required by law. We will not sell health data as a standalone asset.

9. No sale, ad-tech sharing, or restricted-use disclosure of health data

Murph does not sell or rent personal information.

Murph does not sell, rent, license, or otherwise disclose consumer health data, HealthKit data, wearable data, journal data, prompt content, health files, health memories, or derived health insights to data brokers, advertising networks, third-party advertising platforms, or information resellers.

Murph does not "share" health data for cross-context behavioral advertising, targeted advertising, retargeting, lookalike audience creation, attribution, ad measurement, or similar advertising or marketing purposes. Murph does not use health data to create or enrich advertising profiles.

Murph does not disclose health data to employers, insurers, benefits administrators, lenders, credit agencies, or similar parties for eligibility, underwriting, pricing, employment, benefits, credit, or risk-scoring decisions, unless you expressly direct us to do so for a specific feature and applicable law permits it.

No health-facility geofencing for advertising or profiling. Murph does not use geofences around healthcare facilities, reproductive-health facilities, gender-affirming-care facilities, mental-health facilities, addiction-treatment facilities, or similar locations to identify users, infer health status, send advertising, build profiles, or sell/share consumer health data.

We will not apply materially different sale, sharing, targeted-advertising, data-broker, eligibility-decision, or general-purpose model-training practices to previously collected health data unless we first provide required notice and obtain any required opt-in consent or authorization. Nothing in this paragraph limits the no-sale, no-targeted-advertising, no-data-broker, no-eligibility-decision, and no-health-data-training commitments above for current Murph consumer features.

10. Tracking, analytics, and health surfaces

Murph and our service providers may use cookies, local storage, session tokens, and similar technologies to:

- authenticate users;
- keep you signed in;
- remember preferences;
- secure sessions and prevent abuse; and
- operate core website and hosted-service functionality.

Murph may also use analytics or similar tools to understand service performance and usage.

No advertising trackers on health surfaces. We do not intentionally place third-party advertising pixels, retargeting tags, behavioral advertising SDKs, or similar tracking technologies on pages, screens, APIs, or workflows where users enter, view, upload, connect, or receive health data.

No health content in analytics. We do not intentionally send journal content, health prompts, wearable metrics, health-file contents, health-file names, symptoms, diagnoses, lab values, health memories, integration tokens, or health-related URL query strings to analytics or advertising tools.

Analytics limits. Where we use analytics or diagnostics, we configure them to collect minimized operational information such as performance, uptime, feature usage, crash reports, and security events, and to avoid collecting health content where feasible.

If Murph uses non-essential analytics, advertising, or personalization technologies in the future, Murph will provide any disclosures and consent mechanisms required by applicable law.

11. Apple Health, HealthKit, Health Connect, and wearable APIs

If you connect Apple Health, HealthKit, Google Health Connect, wearable providers, device providers, or wellness apps, Murph will collect only the categories of data you authorize and only for the features you enable.

Apple Health / HealthKit. Murph uses HealthKit data only to provide health, fitness, wellness, journaling, personalization, import, export, or other features you request. Murph does not use HealthKit data for advertising, data mining, third-party advertising, cross-context behavioral advertising, data-broker disclosure, insurance/employment/credit decisions, or general-purpose AI model training. Murph does not disclose HealthKit data to third parties except to service providers as necessary to provide or improve the health, fitness, wellness, import, export, sync, or personalization feature you request; for health research with your permission; where required by law; or as otherwise permitted by Apple's rules and applicable law.

Health Connect publication surfaces. If Murph distributes a Google Health Connect integration through Google Play or another app-store surface, the store listing, Health Connect permission flow, and in-product legal links will point users to the same HTML Privacy Policy at withmurph.ai/legal/privacy (https://withmurph.ai/legal/privacy). Murph will request only health and fitness permissions tied to a clear feature benefit, and the Privacy Policy will describe the collected data categories, use, storage, sharing, retention, deletion, and security practices.

Health Connect and wearable APIs. Murph uses data from Google Health Connect, wearable providers, device providers, and wellness apps only to provide the feature you enable; personalize, import, export, sync, summarize, secure, or troubleshoot that feature; or comply with law. Murph does not use that data for advertising, data-broker disclosure, insurance/employment/credit decisions, or general-purpose AI model training.

Permissions and revocation. You can manage some health-data permissions through your device, browser, app, or connected-provider settings. Disconnecting a provider or revoking permissions stops future collection from that provider, but may not automatically delete data already stored by Murph or by independent third parties, unless deletion is required by law or requested through available privacy controls.

12. Research and product improvement

Murph may improve the service using aggregated, de-identified, pseudonymized, or otherwise minimized information where feasible.

No identifiable health research without separate consent. Murph will not use identifiable health data for human-subjects research, clinical research, publication, or sponsored research unless you separately opt in, the use is otherwise permitted by law, or the data has been de-identified as permitted by applicable law.

Research notices. If Murph offers a research feature, the applicable consent or study notice will describe the research sponsor, data categories, purpose, retention period, withdrawal process, whether results may be published, and who controls the research data.

Health Commons contributions. Private experiment runs and notes are private by default. If you choose to contribute an outcome card, protocol note, aggregate result, or similar material to Health Commons, Murph will show the contribution boundary before submission and will process the contribution according to the consent or product notice for that feature. Contributions may be tied to protocol revisions, confidence labels, source-quality labels, and de-identified or aggregate outcome summaries. Do not contribute another person's personal or health information unless you have the required authority and consent.

De-identified data. If Murph maintains de-identified data, Murph will maintain and use it in de-identified form and will not attempt to reidentify it except as permitted by law. We will use reasonable technical and organizational measures to prevent reidentification and require recipients of de-identified data to make similar commitments where required by law.

13. Data retention

Murph retains personal information only for as long as reasonably necessary for the purposes described in this Privacy Policy, including to provide Murph, comply with law, resolve disputes, enforce agreements, maintain security, prevent fraud or abuse, and honor your choices. The table below describes Murph's current retention targets for hosted Murph systems. Actual deletion timing may vary where deletion depends on a user-controlled provider, deployment-specific database backup cycle, legal hold, security investigation, billing/tax obligation, unresolved dispute, or technically constrained backup restoration process.

Category: Account/profile information; Typical retention target: While your account is active and up to 90 days after deletion, unless longer retention is required for legal, security, fraud-prevention, or dispute purposes

Category: Health and user-submitted content; Typical retention target: Until you delete it or your account is deleted; targeted for removal from active hosted systems within 30 days and from backups within 90 days, unless legally preserved

Category: Wearable/device raw sync data; Typical retention target: While the integration is active, or queried on demand where technically supported; targeted for deletion within 30-90 days after disconnect/account deletion unless needed for security, legal, or user-requested features

Category: Health memories, summaries, embeddings, and derived insights; Typical retention target: Until you delete/disable them or your account is deleted; targeted for removal from active systems within 30 days and backups within 90 days unless legally preserved

Category: Integration tokens and credentials; Typical retention target: Until disconnect/account deletion, then targeted for revocation or deletion promptly, normally within 7-30 days

Category: Webhook receipts, routing metadata, and sync logs; Typical retention target: Typically 30-90 days unless needed for security, debugging, replay protection, fraud prevention, reconciliation, or legal preservation

Category: User-visible assistant history containing health data; Typical retention target: Until you delete it or your account is deleted; targeted for removal from active hosted systems within 30 days and backups within 90 days unless legally preserved

Category: Operational prompt/tool traces containing health data; Typical retention target: Not retained by default outside user-visible history; where retained for support, security, abuse prevention, or debugging, targeted for deletion within 30 days unless legal, security, or dispute needs require longer

Category: Support communications; Typical retention target: Typically up to 3 years, with health content redacted or deleted sooner where feasible

Category: Billing/tax records; Typical retention target: As required for accounting, tax, audit, and legal obligations

Category: Security logs; Typical retention target: Typically 90-365 days, with health content excluded where feasible

Category: Backups; Typical retention target: Deleted or overwritten on a rolling basis, typically within 90 days for hosted systems Murph controls

We do not retain health data "just in case." We retain it only for the purposes described in this Privacy Policy, for the periods described above, or as required to comply with legal, security, fraud-prevention, accounting, dispute-resolution, or user-request obligations.

Murph may retain aggregated, de-identified, or otherwise non-identifying information that does not reasonably identify you, provided we maintain and use it in de-identified form as required by law.

14. Security and hosted processing transparency

Murph uses administrative, technical, and physical safeguards designed to protect personal information. These may include, as appropriate:

- encryption in transit;
- encryption at rest for hosted health data and sensitive account data;
- access controls, least-privilege practices, and need-to-know review;
- privacy-preserving identifiers or lookup values for some workflows;
- logging, monitoring, and abuse-prevention controls;
- secure key handling and signed internal requests for certain hosted operations; and
- staff training and vendor management processes.

For hosted health data, Murph applies controls appropriate to the feature and hosting environment, which may include encryption in transit and at rest, role-based access controls, least-privilege access, production-access logging, access reviews, token vaulting or equivalent secure credential handling, secrets management, vendor review, incident-response procedures, and workforce confidentiality obligations. Access to hosted health data is limited to personnel and providers with a need to operate, secure, support, or troubleshoot Murph, and sensitive access may be logged and reviewed.

Hosted Murph may require Murph and its service providers to process readable content when necessary to provide requested features, secure the service, investigate incidents, debug problems, or provide support. Although Murph uses encryption and access controls, Hosted Murph is not a zero-knowledge, operator-blind, or end-to-end-encrypted service unless we expressly say otherwise for a specific feature.

Support access. Murph personnel do not access the contents of your hosted health data for support unless needed to respond to your request, troubleshoot the service, investigate abuse/security issues, comply with law, or protect rights and safety.

HIPAA and Business Associate Agreements. Unless Murph expressly enters into a written Business Associate Agreement with you that identifies covered services, Murph is not acting as your HIPAA business associate, and Hosted Murph is not offered for creating, receiving, maintaining, or transmitting protected health information on behalf of a HIPAA covered entity or business associate. If you are a covered entity or business associate, do not submit PHI to Murph unless we have signed a BAA covering the applicable service and you have configured the service according to any HIPAA-ready implementation requirements we provide. Consumer, beta, experimental, local, self-hosted, non-enterprise, or third-party-integrated features may be excluded from BAA coverage unless the BAA expressly says otherwise.

Security incidents and health-data breach notices. If we identify a security incident involving personal information or health data, we will investigate and take steps to mitigate harm. A health-data breach may include unauthorized access, acquisition, use, or disclosure of unsecured health data, including certain disclosures inconsistent with our privacy promises, not only traditional cybersecurity intrusions. If Murph determines that a security incident triggers a legally required breach notice, including under applicable consumer health data, personal data, health breach notification, or similar laws, Murph will provide notices to affected users, regulators, service providers, or other parties as required by law. Service providers that process health data for Murph must notify us of security incidents as required by contract and applicable law.

If you self-host or run Murph locally, you are responsible for the security of the systems, credentials, backups, and network environments you control.

Local and self-hosted telemetry. If you run Murph locally or self-host Murph, Murph does not receive your local health content unless you connect hosted Murph services, enable telemetry, use a hosted integration, request support, or otherwise transmit information to us. Optional telemetry is off by default for health content and does not include journal entries, prompts, files, health metrics, health memories, wearable data, integration tokens, or other health content unless we clearly disclose the telemetry and obtain any required consent.

No method of transmission or storage is completely secure, and Murph cannot guarantee absolute security.

15. International transfers

Murph and our service providers may process information in the United States and other countries where we or our providers operate. Those countries may have data-protection laws different from those in your jurisdiction.

Where required by law, Murph will use appropriate safeguards for cross-border transfers, such as contractual protections or other approved transfer mechanisms.

16. Your choices and rights

Depending on where you live and subject to applicable law, you may have rights to:

- access personal information Murph holds about you;
- correct inaccurate information;
- delete certain information;
- receive a portable copy of certain information;
- object to or restrict certain processing;
- withdraw consent where processing is based on consent;
- opt out of certain marketing communications; and
- appeal certain privacy-rights decisions.

Depending on how you use Murph, you may also be able to:

- disconnect linked integrations or providers;
- change device, browser, or app permissions;
- manage account settings and preferences;
- delete or revoke certain invite flows or invitations;
- export or copy data directly from local or self-hosted environments you control; or

- request account deletion.

To exercise privacy rights, contact us at legal@justco.build. We may need to verify your identity before fulfilling certain requests. Where allowed by law, you may use an authorized agent to make a request on your behalf. Murph may also deny or limit a request where permitted by law, such as where fulfilling it would infringe the rights of others, undermine security, or conflict with legal obligations.

If we deny a request that is appealable under applicable law, you may appeal by replying to our decision or by emailing legal@justco.build with the subject line "Privacy Appeal."

Murph will not discriminate against you for exercising privacy rights provided by law.

17. Consumer Health Data Notice

Murph maintains a separate Consumer Health Data Notice for disclosures required by U.S. consumer health privacy laws, including the Washington My Health My Data Act and similar laws.

Where that separate notice applies and conflicts with this Privacy Policy, the separate Consumer Health Data Notice controls for consumer health data to the extent required by law.

You can access the Consumer Health Data Notice at withmurph.ai/consumer-health-data-privacy-policy (https://withmurph.ai/consumer-health-data-privacy-policy) or another clearly labeled link we make available on our homepage, in-app settings, and relevant onboarding or data-collection flows.

18. Region-specific disclosures

A. EEA / UK / Switzerland

If applicable, you may also have the right to lodge a complaint with your local supervisory authority.

B. U.S. state privacy laws

If applicable U.S. state law grants you rights relating to access, deletion, correction, portability, opt-out, appeal, or limitation of sensitive-data processing, you may exercise those rights using the methods described above. Murph does not sell or rent personal information and does not use health data you provide through Murph for cross-context behavioral advertising.

If Murph later offers a dedicated online privacy-rights portal or self-serve workflow, this Privacy Policy may be updated to identify that process.

19. Age restrictions and children’s privacy

Murph is not directed to anyone under 18 years old, and we do not knowingly collect personal information from anyone under 18 in a manner not permitted by law. If we learn that we collected personal information from someone under 18 in a manner not permitted by law, we will take steps to delete it.

If a different age threshold, parental consent rule, or other age-related standard applies under applicable law, that law controls.

20. Third-party services and links

Murph may link to or interoperate with third-party services. This Privacy Policy does not govern third-party websites, applications, hardware, wearable providers, identity providers, payment processors, messaging channels, model providers, search providers, or integration providers except as described here for Murph-controlled processing. Please review their privacy policies before using those services.

21. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. When we do, we will revise the "Last Updated" date above and provide any additional notice required by law. Your continued use of Murph after an updated Privacy Policy becomes effective is subject to that updated policy.

22. Contact us

For questions, requests, or complaints regarding this Privacy Policy or Murph’s privacy practices, contact:

Just Cobuild, Co. Privacy Email: legal@justco.build Support Email: legal@justco.build Mail: 2261 Market Street, STE 85230, San Francisco, CA 94114 USA Website: https://withmurph.ai