Healsend Inc. — Master Privacy Policy (U.S.-Only, MSO Model)

Effective Date: October 5, 2025

Healsend Inc.
30 N Gould St Ste R
Sheridan, WY 82801
Email: yourhealth@healsend.com
Website: https://healsend.com

Contents

1. Introduction & Roles

Healsend Inc. ("Healsend," "we," "us," or "our") operates a U.S.-only telehealth technology and administrative services platform. We are a management services organization (MSO) and technology facilitator. We do not practice medicine, dispense medication, or make clinical decisions. Licensed, independent professional entities and their clinicians (collectively, "Professional Entities" or "Providers") deliver clinical services; independent pharmacies dispense prescriptions. This Master Privacy Policy explains how Healsend collects, uses,

discloses, and protects personal information in connection with our websites, applications, and related services (the "Services").

2. Scope; U.S.-Only Audience; No International Use

This Policy applies to users located in the United States. We market only to U.S. residents and do not target or offer the Services to individuals outside the United States. If you access the Services from outside the U.S., you do so at your own initiative and understand your information will be processed in the U.S. This Policy does not apply to third-party websites or services linked from our Services; such third parties are governed by their own policies.

3. Key Definitions

- "Personal Information" means information that identifies, relates to, describes, or could reasonably be linked to a person or household.
- "Consumer Health Data" means personal information linked or reasonably linkable to a consumer that identifies the consumer's past, present, or future physical or mental health status (as defined under certain state laws).
- "Sensitive Personal Information" includes data categories identified by state laws (e.g., precise geolocation, government IDs, health data, biometric identifiers).
- "Protected Health Information (PHI)" has the meaning given in HIPAA when processed by covered entities or business associates for HIPAA purposes.
- "Professional Entities/Providers" are independent medical groups and clinicians who deliver healthcare services; they are not owned or controlled by Healsend.
- "Service Providers/Subprocessors" are vendors that process data under our instructions to support the Services (e.g., hosting, analytics, payments).

4. Categories of Personal Information Collected

Depending on your interactions, we may collect:

- Identifiers (name, postal address, email, phone number, unique IDs).
- Demographics and account credentials (date of birth, login, password).
- Health and clinical intake information you provide to use the Services.
- Financial/transaction data (payment method token, billing details).
- Internet/network activity and device data (IP address, logs, cookies).
- Geolocation (general location derived from IP/device settings).
- Communications (email, chat, support tickets, call/video recordings where permitted).
- Images/media you upload (e.g., photos of IDs or affected areas, if requested).
- Inferences drawn from other data (e.g., risk flags, adherence signals).
- Biometric/sensor data if you choose to use supported devices (see Section 10).

5. Sources of Personal Information

- Directly from you (registration, intake, scheduling, messages).
- Automatically via cookies, SDKs, analytics, and security logs.
- From Professional Entities/Providers and pharmacies involved in your care (where permitted by law).
- From payment processors and logistics providers to complete transactions.
- From publicly available sources and marketing partners where allowed by law.

6. Purposes of Processing

We use Personal Information to:

1. Create and manage accounts; authenticate users; personalize experiences.
2. Facilitate telehealth interactions ("store and forward," live video/audio, secure messaging).
3. Enable prescription processing and fulfillment with pharmacies.
4. Process payments; manage membership/subscription billing and receipts.
5. Provide support; respond to inquiries; conduct quality assurance and training.
6. Detect, investigate, and prevent fraud, abuse, or security incidents.
7. Conduct analytics, improve performance, and develop new features.
8. Comply with law, respond to legal process, and enforce our terms and policies.
9. Perform or obtain audits, compliance assessments, and risk evaluations.
10. With your consent, conduct additional uses disclosed at the time of collection.

7. Our Role as MSO/Technology Provider; Provider Role

Healsend is not a medical provider. We facilitate communications and data flows between you and the Professional Entities. Clinical decisions are made solely by Providers. Healsend may process certain data on behalf of Professional Entities subject to written agreements; those data are controlled by the Professional Entities.

8. HIPAA/HITECH Boundary; Business Associate Arrangements

Some information processed within provider–patient encounters may constitute PHI under HIPAA when handled by covered entities (e.g., Professional Entities or pharmacies) or their business associates. Healsend may act as a business associate pursuant to a Business Associate Agreement (BAA) for defined services. Outside of those HIPAA contexts, information collected by Healsend is governed by applicable state consumer privacy laws and this Policy.

9. Consumer Health Data (WA MHMDA; NV SB370)

For residents of states with consumer health data laws (e.g., Washington's My Health My Data Act; Nevada SB370), Healsend implements consent, access, deletion, and restrictions on

secondary use of Consumer Health Data as required. We do not sell Consumer Health Data and restrict advertising-related uses consistent with these laws.

10. Biometric & Sensor Data (e.g., BIPA/TX/WA)

If you enable features that capture biometric identifiers or use connected health sensors, we will provide or request appropriate notices and consents, use such data only for the disclosed purposes, protect it with reasonable safeguards, and retain it no longer than necessary or as required by law.

11. Sensitive Personal Information

We handle Sensitive Personal Information (including health data, precise geolocation, and government IDs) with enhanced controls, limit internal access on a need-to-know basis, and, where required, limit use to necessary service delivery purposes unless you provide consent for additional uses.

12. Cookies, Tracking, and Global Privacy Control (GPC)

We use cookies and similar technologies for functionality, security, analytics, and limited marketing. Browser tools allow you to block or delete cookies; some features may be limited. Where required, we honor browser-based Global Privacy Control signals as an opt-out of certain tracking-based processing. See Appendix F for details.

13. Targeted Advertising, Analytics, and Opt-Outs

We do not sell Personal Information for money. Certain analytics/advertising uses may be deemed "selling" or "sharing" under state laws. You may opt out of such processing as described in Sections 18–20 and Appendix F, or by contacting yourhealth@healsend.com.

14. Disclosures to Providers, Pharmacies, Service Providers, and Others

- Professional Entities/Providers — to facilitate care, scheduling, and communications.
- Pharmacies — to fulfill prescriptions and manage delivery logistics.
- Service Providers/Subprocessors — hosting, storage, analytics, payment, customer support; bound by contracts limiting use.
- Affiliates and professional advisors — for governance, audit, and compliance.
- Authorities and legal process — as required by law or to protect rights, safety, and security.
- Business transfers — in connection with mergers, acquisitions, or reorganization.

15. Retention & Disposal (with Retention Schedule)

We retain Personal Information only as long as necessary for the purposes in this Policy, considering legal, regulatory, and operational needs (e.g., fraud prevention, tax/audit). See Appendix B for retention periods by category and disposition methods.

16. Security Program (Administrative, Technical, Physical Safeguards)

- Administrative: policies, training, vendor due diligence, access reviews, risk assessments.
- Technical: encryption in transit and at rest where appropriate, MFA for privileged access, network segmentation, logging/monitoring.
- Physical: data center controls, device management, secure media handling.
- Testing: vulnerability scanning and periodic assessments proportionate to risk.

17. Incident Response & Breach Notification (High-Level Summary)

We maintain an incident response plan. Upon discovery of a potential incident, we investigate, contain, and remediate. If required by law, we notify affected individuals and regulators within applicable timelines. See Appendix D for workflow summary.

18. Patient/Consumer Privacy Rights (General U.S. Rights)

- Access and obtain a copy of certain Personal Information.
- Request correction of inaccurate Personal Information.
- Request deletion, subject to legal exceptions (e.g., recordkeeping, fraud prevention).
- Opt out of targeted advertising or certain profiling/analytics where applicable.
- Appeal a decision regarding your privacy request.

To exercise rights, contact yourhealth@healsend.com. We will verify your identity using reasonable methods and respond within legally required timelines.

19. California Privacy Rights (CCPA/CPRA)

- Right to know/access, delete, correct, and data portability.
- Right to opt out of selling/sharing and to limit use of Sensitive Personal Information where applicable.
- No discrimination for exercising rights.
- Notice of categories collected, purposes, sources, recipients, and retention (see Sections 4–6, 14–15).

20. Other State Privacy Rights (CO, CT, DE, IA, MT, NE, NH, NJ, NV, OR, TX, UT, VA, etc.)

Residents of these states may have similar rights (access, correction, deletion, portability, opt-out of targeted advertising) and an appeal right. We will honor verified requests consistent with state law.

21. Children's & Minor's Privacy

The Services are intended for adults 18+. We do not knowingly collect Personal Information from minors. If we learn a minor has provided information, we will delete it. Contact yourhealth@healsend.com for assistance.

22. Marketing, SMS/Text, and Email Communications

We may send transactional and, with consent where required, marketing messages. You can opt out of marketing emails via the unsubscribe link or by contacting yourhealth@healsend.com. For SMS, you can reply STOP to opt out. Message and data rates may apply.

23. Financial & PCI Matters

Payments are processed by third-party processors who may act as independent controllers of your payment data. We receive limited tokens/metadata to reconcile transactions. PCI DSS obligations are handled by the processor.

24. Controlled Substances; 42 CFR Part 2

If a Provider prescribes controlled substances, applicable DEA and state laws apply. If substance-use disorder information is involved, 42 CFR Part 2 may restrict disclosure by the Provider or program.

25. Accessibility & Non-Discrimination

We strive to make the Services accessible and to provide reasonable accommodations. We do not discriminate based on protected characteristics and comply with applicable laws.

26. Automated Decision-Making & AI Use

We may use algorithms to route intake forms, detect fraud/abuse, and prioritize support. We do not use automated decision-making to deny medical care. You may request information about our use of automated tools and opt out of non-essential profiling where state law provides.

27. Telehealth "Store and Forward"; Cross-Entity Data Flows

We may use asynchronous ("store and forward") technology to transmit your information to Providers for review. Healsend facilitates the secure transfer of information but does not provide clinical care. Providers determine what information is clinically necessary.

28. Data Subject Request Process & Verification

- Submit requests to yourhealth@healsend.com with your name, contact details, and the rights you seek to exercise.
- We may request additional information to verify identity and protect against fraud.
- Authorized agents may submit requests where permitted by law with sufficient authorization.
- We maintain records of requests and outcomes in accordance with retention obligations.

29. Changes to this Policy

We may update this Policy from time to time. If we make material changes, we will post the updated Policy and update the Effective Date. Your continued use after the Effective Date indicates acceptance.

30. Contact Information

Healsend Inc.
30 N Gould St Ste R
Sheridan, WY 82801
Email: yourhealth@healsend.com
Website: https://healsend.com

Appendix A — Data Inventory & Categories

This appendix maps data categories to examples and typical sources.

- Identifiers — Name, email, phone; Source: user-provided.
- Health Intake — Symptoms, history, images; Source: user-provided; may become PHI with Providers.
- Transaction — Payment tokens, order details; Source: payment processors and platform.
- Technical — IP, device IDs, logs; Source: automatic collection.
- Communications — Chats, emails, recordings; Source: user interactions.

Appendix B — Retention Schedule

Retention periods are subject to legal, regulatory, and operational needs. Examples:

- Account & identifiers — For the life of the account + up to 7 years after closure (fraud, audit).
- Health intake (non-PHI) — Minimum necessary for service delivery; typically 7 years unless law requires longer.
- Payment tokens/metadata — 7 years for financial recordkeeping.
- Logs & security events — 12–24 months depending on risk and legal needs.
- Record of privacy requests — 24 months or as required by state law.

Appendix C — State Privacy Rights Summary

Quick reference to common rights under comprehensive state privacy laws (actual rights depend on residency and exclusions):

- Access/Know, Correct, Delete, Data Portability, Opt-Out of Targeted Advertising.
- Appeal rights if a request is denied.
- Limitations/exemptions apply (e.g., HIPAA data, GLBA data, employment records).

Appendix D — Incident Response & Notification Workflow

- Detect & triage → contain → investigate root cause → assess impact and legal triggers.
- Notify affected parties and regulators when required by law within applicable timelines.
- Remediate vulnerabilities; document lessons learned; update controls.

Appendix E — Service Provider/Subprocessor Standards

- Contractual data protection terms; use limitation; confidentiality; breach notice duties.
- Security controls commensurate with risk (encryption, access control, logging).
- Subcontractor flow-down obligations; audit/attestation (e.g., SOC 2/ISO 27001).
- Data return/deletion at end of engagement; assistance with rights requests where applicable.

Appendix F — Cookies & Tracking Technologies

- Strictly necessary cookies — authentication, security, session management.
- Functional cookies — preferences, site performance.
- Analytics — usage metrics to improve Services (with opt-out options).
- Advertising/retargeting (limited use) — opt-out mechanisms and GPC signals honored where required.
- Controls — browser settings, platform preferences, and email to exercise rights.