Privacy Policy

Effective Date: October 15, 2025

Aspect Health Global Inc.
919 North Market Street, Suite 950, Wilmington, DE 19801, USA
Contact: support@aspect-health.com

1. Overview & Scope

This Privacy Policy explains how Aspect Health Global Inc. (“Aspect,” “we,” “us,” or “our”) collects, uses, discloses, and safeguards personal information in connection with our non-clinical wellness program and related services (the “Program”). The Program is intended solely for general wellness, self-education, and lifestyle support. It is **not** medical care, diagnosis, or treatment, and is **not** a substitute for professional medical advice or healthcare. No aspect of the Program is intended to diagnose, treat, cure, or prevent any disease or medical condition.

Not HIPAA-Covered: Aspect is not a “Covered Entity” under the U.S. Health Insurance Portability and Accountability Act (HIPAA), and therefore HIPAA regulations do not apply to the information you provide to us. However, we are committed to protecting your privacy in compliance with applicable laws (including California’s CPRA and other U.S. state privacy laws listed below), and in alignment with core principles of the EU/UK GDPR where relevant. By using our Program or providing us with personal information, you acknowledge that you have read and agree to this Privacy Policy. If you do not agree, please do not use the Program.

Scope: This Policy covers personal information we collect through our websites, mobile applications, devices, and services related to the Program. It does not cover any third-party websites or services that may be linked to our services, nor any information handled by third-party health care providers. Our Terms of Service and Post-Purchase Consent and Acknowledgement Agreement may provide additional terms regarding your use of the Program. In the event of a material change to this Policy, we will seek your consent if required and/or provide notice as described below.

2. Information We Collect

We collect personal information (also referred to as “Personal Data”) that you voluntarily provide to us, that is generated through your use of our services, or that we obtain from third-party sources (such as integrated device vendors or analytics providers). The categories of personal information we collect include, but are not limited to, the following:

- **Contact and Account Information:** Identifiers such as your name, email address, telephone number, postal address, date of birth, login credentials, and other information you provide when you sign up or communicate with us.

- **Eligibility and Health Screening Information:** Certain health or personal details collected at enrollment to ensure you meet our Program eligibility criteria. This may include confirmation that you are over 18 and not in an excluded category (e.g. not insulin-dependent, not undergoing dialysis, no history of severe hypoglycemia unawareness, and not currently pregnant), as well as general wellness background information you choose to share. We collect this information only to determine your eligibility and safety for Program participation.

- **Health & Wellness Data (including CGM Data):** Health-related information you provide or that is collected during the Program. This includes data from Continuous Glucose Monitoring (CGM) devices (e.g. glucose readings), other biometric or wellness data (such as diet logs, exercise or activity data, sleep or mood information), and any data you choose to sync from health or fitness apps and devices (for example, Apple HealthKit, Google Fit, wearables, etc.). **Important:** Any CGM or health data we collect is for your informational and educational purposes only as part of the wellness Program, and not for medical diagnosis or treatment.

- **Session Recordings and AI-Generated Notes:** With your consent, we may record coaching sessions (audio and/or video) and use AI-assisted tools to transcribe and summarize these sessions. This may include audio/visual recordings of your voice or image during coaching calls and the textual notes or summaries generated by our in-house AI systems from those sessions. (See Section 5 below for more on how these recordings and AI notes are handled.)

- **Usage Data and Device Information:** Information about your device and how you interact with our services. This includes technical identifiers and online activity information such as your IP address, device type, operating system, browser type, app version, unique device identifiers (e.g. UUID), cookie IDs, pages or screens viewed, features used, dates/times of visits, and crash or diagnostics information. We may also collect approximate location information (e.g. city or region) inferred from your IP address or device settings, to personalize content (such as time zone or local offerings). Precise geolocation is not collected or tracked, and we do not access your device's GPS without your explicit permission.

- **Communications and Support Data:** The content of your communications with us, such as emails, chat messages, survey responses, or customer support inquiries, and related contact details. If you call our support line, we may record the call (with notice to you) for training and quality assurance.

- **Payment and Transaction Information:** If you purchase the Program or other services, we (or our third-party payment processors) collect payment information such as your payment card details, billing address, and transaction history. *Note:* We do not store full credit/debit card numbers ourselves; payments are handled securely by accredited payment processors (e.g. Stripe) on our behalf. We retain limited transaction details (e.g. your name, contact, the amount and date of transaction, last four digits of your card or token, and payment method) for recordkeeping and to manage subscriptions, refunds, or disputes.

We may also collect **aggregated, de-identified, or anonymized data** that is not reasonably linked to an identified individual. Such data is not considered personal information under this Policy, and we may use it for any legitimate purpose. **You are responsible for ensuring that any personal information you provide is accurate and up-to-date.** If you choose not to provide certain information, some features of the Program may not be available or work as intended.

3. Notice at Collection of Personal Information

Below is an overview of the categories of personal information we collect (as described in Section 2), along with the sources from which we collect it, the purposes for which we use it, whether we "share" it for cross-context behavioral advertising, the types of recipients with whom we disclose it, and our retention period for each category. This *Notice at Collection* is provided in accordance with the California Privacy Rights Act (CPRA) and other similar state laws. **We do not sell your personal information** (no monetary exchange for data); and we only "share" personal information for targeted advertising as indicated below.

- **Contact & Account Identifiers** (e.g., name, email, phone, account ID)
    - **Examples:** Full name, email address, phone number, mailing address (if provided), account username/ID
    - **Sources:** Directly from you (during signup or communications); from your device (for IP address)
    - **Purposes:** To register and manage your account; to communicate with you (service messages, updates, customer support); to verify your identity and prevent fraud; **Marketing:** to send promotional emails or newsletters (if you opt-in); to comply with legal obligations (e.g. billing, audit)
    - **Shared for Ads?:** No (we do not share contact details for third-party advertising)
    - **Recipients:** Service providers (e.g. cloud hosting, CRM/email delivery vendors, fraud prevention services); business operations platforms (e.g. customer support

software); our authorized personnel (staff and coaches). *[We do not disclose contact info to independent third-party controllers except with your consent or as required by law.]*

- **Retention:** For the duration of your account, plus up to 3 years after account deletion (to handle inquiries, legal obligations, or reactivation requests). Transaction records may be kept up to 7 years for tax and accounting compliance.

- **Eligibility & Health Screening Info** (Program intake data)
  - **Examples:** Age/date of birth; self-reported health status (e.g. confirmation of non-insulin use, not pregnant, etc.); relevant medical history for eligibility (e.g. no dialysis, no severe hypoglycemia episodes)
  - **Sources:** Directly from you (pre-enrollment questionnaires or forms)
  - **Purposes:** To confirm you meet eligibility requirements for the Program and ensure safety; to tailor the Program to your profile (e.g. coaching considerations based on your background). *Note:* This information is **not** used for marketing or advertising purposes.
  - **Recipients:** Service providers assisting with enrollment or secure data storage; our authorized personnel (Program administrators, coaches) who need to know for safety. *[Not disclosed externally unless required for legal compliance or safety reasons.]*
  - **Retention:** Retained as long as necessary for the enrollment decision and your participation. For accepted participants, kept with your account data during active enrollment. If you do not enroll or are deemed ineligible, we delete this information after 30 days (except for a record of the ineligibility reason, kept up to 1 year).

- **Health & Wellness Data** (incl. CGM data and other sensitive personal data)
  - **Examples:** CGM sensor readings (glucose levels); nutrition and diet logs; exercise, activity, or sleep data; other wellness metrics you choose to track (heart rate, weight, etc.); health journal entries or survey answers
  - **Sources:** From you directly (through app inputs, questionnaires, or during coaching sessions); from devices or apps you connect (e.g. CGM device data transmitted via its app or our app; data imported from Apple Health or Google Fit with your permission)

- **Purposes:** To provide the core wellness services (e.g. analyzing your data to give insights, trends, and personalized recommendations); to allow you and your coach to monitor your progress and adjust your plan; to improve the Program (e.g. aggregate analysis for efficacy, feature development — using de-identified data where possible); to troubleshoot device issues (e.g. CGM connectivity) and support your use of integrated devices; **Safety:** to identify potential health warning signs and advise you to seek medical care if needed (we do **not** provide medical treatment, but we may alert you if data indicates a serious issue).

- **Recipients:** Service providers/processors (secure cloud databases and analytics platforms hosting health data; CGM device platform providers acting under our instruction; IT security and backup services); authorized personnel (your coaching team and select staff, bound by confidentiality, who analyze and use the data to assist you). *[We do not disclose identifiable health data to independent third parties unless you direct us to (e.g. you request a data transfer to your doctor) or if required by law.]*

- **Retention:** Maintained for as long as you are an active user of the Program, so we can provide services. You can request deletion of specific health data at any time. Upon account deletion or end of Program, we generally delete or de-identify health data within 90 days, except where retention is required by law or for internal research (in de-identified form). We may retain aggregated, non-identifiable wellness data indefinitely for research and product improvement.

- **Session Recordings & AI Notes** (coaching session audio, video, transcripts, summaries)

    - **Examples:** Audio/video recordings of coaching sessions you participate in; AI-generated text summaries or analyses of those sessions

    - **Sources:** From you and your coach during sessions (recorded **only** with your consent); generated by our internal AI note-taking tools (from session content)

    - **Purposes:** *Service delivery:* to provide you with session summaries and help our coaches review key points from your sessions; *Quality assurance & training:* to internally review and improve coaching quality, and to train our in-house AI models (only with your *opt-in* consent for AI training) in order to enhance our note-taking and support tools; *Record-keeping:* to document what was discussed and agreed upon in sessions for your reference and our internal accountability.

    - **Recipients:** Service providers (secure cloud storage for recordings; transcription or AI processing services bound by contract to use data only for us, if applicable); authorized personnel (limited Aspect staff such as supervisors, coach trainers, or engineers improving our AI, all under strict access controls).

- **Retention:** Session recordings and AI-generated notes are retained for a limited period. Raw session recordings and transcripts are stored securely for up to 1 year from the date of the session (subject to extension only if reasonably necessary for internal training or legal obligations). After that, recordings are deleted or irreversibly de-identified. If you withdraw consent earlier, we will stop recording and will delete existing identifiable recordings upon your request (allow up to ~30 days to complete deletion).

- **Device, Usage & Analytics Data** (online activity information, cookies, etc.)

  - **Examples:** Device identifiers (UUID, advertising ID); IP address and general location; cookie IDs and tracker data; app usage events (pages viewed, buttons clicked); error/crash logs; dates and times of visits; other browsing or interaction details

  - **Sources:** Automatically collected from your browsers or devices when you use our website or app (via cookies, pixels, SDKs, and server logs); collected via third-party analytics and advertising tools (e.g. Google Analytics, Firebase, Amplitude, Facebook Pixel) that are integrated into our site/app

  - **Purposes:** *Service functionality:* to ensure our website/app functions properly (e.g. remembering preferences, load balancing); *Analytics:* to understand user engagement, troubleshoot issues, and improve our products and marketing (e.g. which features are most used); *Personalization:* to customize your experience (such as content language, or suggesting relevant features); *Advertising/Marketing:* to provide you with relevant marketing for our services, including retargeting or "lookalike" advertising on third-party platforms (with appropriate notice and opt-outs); *Security:* to detect and protect against fraud or malicious activity on our services

  - **Shared for Ads?:** Yes (to the extent this data is collected by third-party cookies and ad/analytics partners for targeted advertising, it is considered "sharing" under CPRA. You can opt out – see Section 7)

  - **Recipients:** Analytics providers (e.g. Google Analytics, Amplitude) and advertising partners (e.g. Meta/Facebook, Google Ads) that collect this data on our site/app via cookies or SDKs – these parties may act as independent controllers of usage data for their own analytics/ad purposes; service providers (IT hosting, infrastructure, and analytics services that process usage data on our behalf under contractual limits). *[We do not sell this information, but some is shared with third parties as described for ads/analytics.]*

  - **Retention:** Retention varies by data type and is often managed by our partners' technology. Cookies and similar trackers have varying lifespans (from the session

duration to ~2 years) unless cleared by you. We generally retain raw usage logs for approximately 1 year. Aggregated analytics data may be kept longer for trend analysis. Advertising identifiers may be retained up to 2 years for ad campaign attribution and are then deleted or de-identified.

- **Communications & Support Data**
    - **Examples:** Customer support inquiries (emails, chat transcripts, or call recordings); survey responses or feedback forms; newsletter email interaction data (e.g. open/click rates)
    - **Sources:** Directly from you when you contact us or respond to surveys; automatically via our email service provider for email interactions (e.g. whether you opened a message)
    - **Purposes:** To respond to your requests and provide customer support or technical assistance; to improve our services based on feedback (e.g. addressing issues, enhancing features); to keep records of your requests and our responses; if you sign up for marketing communications, to tailor and send you such communications (you can unsubscribe at any time)
    - **Shared for Ads?:** No
    - **Recipients:** Service providers (customer support platforms for managing tickets; email delivery services; survey tools – all acting on our instructions); authorized personnel (support agents, customer success and product teams who handle your inquiries). *[We do not disclose support or survey content outside our organization, except anonymized feedback for testimonials with your consent.]*
    - **Retention:** Support communications are retained for as long as necessary to resolve your issue and for up to 2 years for quality assurance and training. Marketing email data is retained until you unsubscribe, or for up to 2 years after an email campaign (unless earlier deletion is requested). Call recordings (if any) are typically kept for ~90 days unless needed longer for training or legal purposes.

Note: The above retention periods may be extended as required or permitted by law (for example, to comply with financial recordkeeping laws or litigation holds), or shortened if you exercise your rights to deletion (see Section 9). When retention periods expire, we will either securely delete the personal information or anonymize it in accordance with applicable laws. We will not use personal information for materially new purposes without providing you notice and obtaining your consent as required.

4. How We Use Personal Information

We use the personal information we collect **only** for the purposes described in this Policy or as otherwise disclosed to you at the time of collection. We do not use your information for any purposes that are incompatible with our commitments to you or beyond what you have consented to. In particular, we may use (process) your personal information for the following business and operational purposes:

To Provide and Improve the Program: We process your information to deliver our services to you – for example, creating your user account; enabling the CGM device integration and displaying your glucose data; facilitating coaching sessions; and generating personalized insights or recommendations. We also use data to improve and enhance the Program's quality, features, and user experience. For instance, we may analyze aggregated user trends or feedback to refine our coaching approach or technology. *(Any use of your data for improving our AI features or training our models is done in-house and only with appropriate consent when required.)*

To Communicate with You: We use your contact information to send you administrative communications about your account or the Program (e.g. appointment reminders, service updates, security alerts, and changes to terms or policies). If you have opted in to marketing communications, we may also send you newsletters or promotions about new features or offers (you can opt out of these at any time). Additionally, we respond to your inquiries, complaints, and requests through email, chat, or phone as appropriate.

For Service Operations and Customer Support: Your information helps us provide customer support, troubleshoot issues, and ensure the functionality and security of our services. This includes using data to debug problems, monitor uptime and performance, and personalize in-app help. For example, if you report a technical problem, we will use relevant data (like device and usage info) to diagnose and fix the issue.

To Ensure Safety and Compliance: We may use personal information (particularly health-related data) to monitor for signs that the Program may not be appropriate or safe for you, consistent with our non-clinical nature. For example, if your CGM readings or feedback suggest a potential medical concern, we might alert you that you should consult a physician (while not diagnosing or treating the issue ourselves). We also process data as needed to meet our legal obligations, such as maintaining transaction records for financial regulations, complying with court orders or lawful requests, and enforcing our contracts (e.g. Terms of Service).

Research and Development: In addition to improving current services, we may use data in de-identified or aggregated form to conduct research on wellness and metabolic health, or to develop new products and services. For example, aggregated CGM trends across users might inform future program content or publications. We will not publicly disclose any research findings in a way that identifies you without your explicit permission. (If we ever wish to use identified

data for research beyond internal program development, we would seek your informed consent.)

Advertising and Marketing (Limited): We do **not** use any sensitive personal information (such as health data or session content) for advertising purposes. We may, however, use limited personal information such as your usage data or cookie identifiers to **retarget** you with ads about our services on third-party platforms — for example, showing an Aspect Health ad on Facebook to people who visited our website. We may also use your email to deliver ads to you on other platforms in a hashed, privacy-protected manner (as part of custom audience features), but only in compliance with applicable law. All such activities are considered "sharing" under California law, and you have the right to opt out of them (see Section 7 and Section 9 for how to opt out). Importantly, we do **not** sell personal information to third parties for money.

With Your Consent (for Other Purposes): If we ever need to use your personal information for a purpose that is not covered by this Privacy Policy, we will describe the new purpose and request your consent before proceeding. For example, if we want to feature your success story on our website, we would seek your permission to use your personal details or testimonial.

We strictly limit the use of personal information to what is necessary and proportionate for the purposes above. We do not use Sensitive Personal Information (as defined by CPRA and other laws, which includes data like health information, precise geolocation, etc.) for purposes other than those allowed by law or with your consent. Specifically, any sensitive data we collect is used only to provide you the services you have requested (wellness coaching and related support), to ensure Program integrity and safety, or as otherwise required by law. If you believe we are using your data in a manner not consistent with these purposes, please contact us at **support@aspect-health.com** so we can address your concerns.

5. AI Note-Taking & Session Recordings

As part of our commitment to provide a high-quality coaching experience, Aspect offers AI-assisted note-taking and session recording features. This section explains how these features work, how we use the information, and the choices you have.

AI-Assisted Notes and Session Recordings: With your express consent, we may record your coaching sessions (which could be conducted via video call, voice call, or even in-person sessions if applicable) and use an artificial intelligence tool to transcribe and summarize the session. The AI note-taking system may capture the audio and/or video of the session and generate a written summary or analysis of key points (for example, action items or insights discussed). These recordings and AI-generated notes are used solely for your benefit and for internal purposes – to help you remember session details, to aid our coaches in tracking your progress, and to allow Aspect to maintain high coaching standards through review and training. Any such recording will be done transparently, and you have the right to decline or stop recording at any time.

Opt-In and Consent: *Session recording and AI processing are optional and require your opt-in consent.* When you joined the Program, you were asked to consent to AI-assisted note-taking and session recordings. If you do not consent, or if you withdraw your consent later, you will still receive the coaching services – there is no penalty or loss of core functionality, except that we will not record or auto-summarize your sessions. You can change your preference at any time by contacting us or updating your settings, and your choice will apply to future sessions.

Purposes of Use: The content of recorded sessions and AI notes is used only for the following purposes (which align with what was presented at consent):

- **Providing Summaries to You:** We may share the AI-generated session notes with you through our app or email so that you have a written recap of what was discussed (e.g. goals set, tips given by your coach). These notes are for your personal use in the Program.

- **Supporting Coaches:** Our coaches may review the recordings or AI transcripts to refresh their memory of your situation and to ensure continuity between sessions. This helps them maintain accuracy and quality in guiding you.

- **Service Improvement and Training:** Internally, a limited number of authorized Aspect personnel (such as senior coaching staff or program developers) may access session recordings and transcripts to monitor service quality, train new coaches (e.g. by reviewing anonymized examples of coaching sessions), and improve our AI note-taking system. If you have opted in to allow your data to train our in-house AI models, we may use some transcripts or recordings to refine our algorithms that power the note summaries or other AI-driven features. This training is done in-house – we do **not** share your identifiable recordings with third-party AI companies for their independent use. All personnel accessing recordings are bound by strict confidentiality obligations.

- **Record-Keeping:** Recordings serve as an accurate log of interactions, which can be useful in resolving any disputes or misunderstandings about what advice was given. They also let us verify compliance with our coaching guidelines.

Protection and Retention: Session recordings and AI notes are treated as highly sensitive information. We store them in encrypted form on secure servers and restrict access to only those with a need-to-know (as described above). We do not use session content for any marketing or advertising purposes, and we do not disclose it outside of Aspect (unless compelled by law, such as in response to a valid subpoena — and even then we will seek to notify you if permissible). We retain recordings and AI-generated content for a limited duration – generally, up to one (1) year – after which they are deleted or anonymized, unless we are legally required to keep them longer. We may keep the AI-generated textual summaries longer than raw video/audio, but only in a form that is not directly identifying, and only for internal reference or improvement of our services. If you withdraw consent or leave the Program, we will promptly cease any further recording, and you may request deletion of existing recordings. (Allow us a

reasonable period to fulfill deletion, as we may need to ensure none of the data is required for legal record-keeping.)

Your Choices: Participation in recorded/AI-summarized sessions is voluntary. If you have concerns about a particular session being recorded, please inform your coach and we will disable recording for that session. You can also request that we delete specific session records if you have privacy concerns; we will evaluate and honor such requests to the extent consistent with our legal and operational obligations. Even if you initially consented, you may contact us at any time to opt out of further recordings or AI processing. We want you to feel comfortable, so we will accommodate your preferences and ensure you still receive a great coaching experience.

6. Health & CGM Data Practices

Aspect recognizes that much of the data we handle – especially Continuous Glucose Monitor (CGM) readings and other health-related information – is highly sensitive. Protecting this information is our top priority. This section details how we handle health data, the roles of any vendors involved in processing it, the control you have over your health data, and the enhanced safeguards we apply.

Collection and Use of Health Data: We collect health data directly from you (e.g. information you log about diet or symptoms) and from devices you integrate, such as CGM sensors. If you use a CGM provided through our Program, the sensor will continuously measure glucose levels. Those readings may be transmitted to our app or servers either via the CGM manufacturer's platform or through an integration we provide. We use your health data strictly to support your wellness journey – for example, to show you trends in your glucose levels, to help our coaches understand your metabolic responses, and to personalize recommendations (like nutritional or lifestyle guidance). We do not use your health data to make medical diagnoses or treatment decisions; any insights provided are for wellness purposes only and are not medical advice. Always consult a healthcare professional for medical interpretation of health metrics.

Third-Party Vendors and Their Roles: We partner with certain vendors to facilitate the collection and processing of health data:

- **CGM Device Providers:** If a CGM is part of your Program, it may be manufactured by a third party (for example, Abbott, Dexcom, or others). That manufacturer might have its own app or cloud service that collects your raw glucose data. In some cases, our app may pull data from the manufacturer's service via an API, or you might use login credentials to allow our access. These CGM providers act as *service providers (processors)* to Aspect when handling your data for our Program purposes. We have agreements in place (or rely on their standard terms) to ensure your data is protected. *(Please note: You may also be subject to the CGM provider's own privacy policy when using their device/app. We encourage you to review those policies, though we will only*

use the data as described herein.)

- **Data Integration Services:** If you choose to link other health apps (like Apple HealthKit or Google Fit) or wearables, those platforms (Apple, Google, Fitbit, etc.) facilitate data transfer. They typically act on your behalf when sending data to us (meaning you authorize them to share your data). We treat any such incoming data the same as other health data — Aspect becomes the controller of that data once we receive it, and we handle it under this Privacy Policy.

- **Cloud Storage and Processing:** We use secure cloud infrastructure (for example, Amazon Web Services or Google Cloud) to store health data. These providers are data processors for us, meaning they store and process data only per our instructions and implement strong security measures.

- **Analytics Tools:** On occasion, we might use specialized analytics on de-identified or aggregated health data to understand overall program efficacy. Any vendor tools for such analysis will either use only anonymized data or operate under our control without any rights to use the data beyond providing the service to us. We do not allow our vendors to use identifiable health data for their own purposes.

User Control Over Health Data: You remain in control of your health and CGM information. Here are key points about your control:

- **Access and Portability:** You can access your health data through our app dashboard. You may also request a copy of your health data in a portable format (for example, a CSV file of your CGM readings) by contacting us. We will provide this data to you (after verifying your identity) as part of your privacy rights (see Section 9).

- **Consent for Sensitive Data:** Under various privacy laws, processing of sensitive personal data (like health data) often requires your consent. By enrolling in the Program and agreeing to our Post-Purchase Consent and this Privacy Policy, you have given us consent to process your health information for the defined Program purposes. You have the right to withdraw that consent at any time. If you do so, we will stop processing your health data going forward (except to the extent necessary to preserve health/safety or as required by law). Note that ceasing processing of health data may affect your ability to continue with the Program (since health data is central to our services), but we will discuss options with you if this situation arises. We will not use your health data for any new purposes without first obtaining your explicit consent.

- **Deleting or Disconnecting Data:** You can request deletion of specific health data points or entire categories of health data. For example, if you wish to remove a particular day's CGM log or a note you provided, we will do our best to accommodate (unless we need to keep it for legal reasons). If you disconnect a device or integration (such as revoking our access to your Apple HealthKit data), we will stop receiving new data from

that source. You may also delete the data from within that third-party app, but note that doing so might not automatically delete data we already received; therefore, please also request deletion from us if desired.

- **Opt-Out of Research Use:** As mentioned, any external research use of your data would be with consent. We might internally use de-identified health data for improving our services, but if you object to even internal R&D use, you can let us know and we will restrict your data from such projects to the extent feasible.

Enhanced Safeguards: We apply strict safeguards to all personal information, but we recognize health data deserves an extra level of protection due to its sensitive nature. Some of the enhanced measures we take include:

- **Encryption:** Your health and CGM data is encrypted both in transit (e.g. via HTTPS) and at rest on our servers. This means that even if data were intercepted or our databases were accessed without authorization, the information would be unreadable without the proper decryption keys.

- **Access Controls:** Only a limited subset of Aspect's team can access identified health data, and always on a need-to-know basis. Coaches only see the data of their own participants. All access to sensitive data is logged and monitored, and we enforce authentication measures (like multi-factor authentication) for any system with health data.

- **Segmentation:** We store health data in specialized, secure environments separate from less sensitive data. For instance, coaching session notes and CGM readings are stored in databases with more restricted access policies than, say, general website analytics data.

- **Training & Policies:** All staff and contractors who handle participant data are trained in confidentiality and data protection practices. Those handling health data receive additional instruction on safeguarding it and understanding the legal requirements (such as not disclosing it improperly). We have internal policies and periodic compliance checks to ensure these standards are upheld.

- **No Unauthorized Sharing:** We do not share your health information with advertisers, social media platforms, or any third parties for their own use. We will resist any attempt to obtain such data from us for other purposes, unless legally compelled. In the rare case we are required by law (e.g. via a court order or subpoena) to disclose health-related information, we will notify you in advance whenever possible and permissible, and only disclose the minimum necessary.

By participating in our Program, you acknowledge that we will collect and use your health-related data as described, and you trust us to keep it secure and used only for your benefit. We take this responsibility very seriously.

7. Cookies, Tracking, and Online Advertising

We and our third-party partners use cookies and similar tracking technologies to provide our online services and to understand and improve your experience. This section describes how we use these technologies, how they relate to advertising, and how you can manage your preferences. (This section also provides notices for U.S. state residents about "sharing" for targeted advertising and your opt-out rights.)

Cookies and Similar Technologies: Cookies are small text files stored on your browser or device to save information. We use first-party cookies (set by Aspect) for things like keeping you logged in, remembering your preferences (e.g. language or dark mode settings), and gathering analytics about usage of our site. We also allow certain third-party cookies or SDKs on our site/app from service providers and partners, which may include:

- **Analytics Cookies/SDKs:** For example, Google Analytics, Firebase, or Amplitude, which help us understand how users navigate our site or app (which pages are visited, for how long, etc.). We use this information to debug issues and make improvements. These analytics services may set their own cookies or device identifiers. The data they collect (like your IP or device info) may be transmitted to and stored on their servers. We configure these tools, where feasible, to limit data collection or use (for instance, enabling IP anonymization in Google Analytics). We do not allow them to use the data for purposes beyond providing services to us.

- **Advertising and Social Media Cookies:** For example, the Facebook Pixel or Google Ads tags. These trackers collect information about your browsing behavior on our site (and may combine it with information from other sites) to help us display targeted advertisements for our Program on other platforms and to measure ad campaign effectiveness. For instance, the Facebook Pixel lets us show an Aspect Health ad on Facebook to people who visited our site or to find similar audiences ("lookalike" targeting). These advertising cookies may also enable third parties (like Facebook/Meta or Google) to gather data about you over time and across different websites. In some cases this is considered a "sale" or "sharing" of personal information under certain laws (like CPRA), even if we do not exchange money.

CPRA "Sharing" Status: Under the California Privacy Rights Act (and similarly under laws in Colorado, Connecticut, Virginia, etc.), allowing third-party advertising cookies or pixels on our online services may be deemed *"sharing"* personal information for cross-context behavioral advertising. This is because those third parties might use the data (e.g. your device identifiers or browsing activity) to profile you and serve ads outside our direct control. We want to be

transparent that we *do* engage in such “sharing” for advertising purposes, limited to the cookie and tracking data described above. We do **not** share or sell any sensitive personal information (such as health or medical data) for advertising. We also do not sell any personal information for monetary consideration. Our only disclosures of data to third parties occur either as service providers/contractors in support of our operations, or as described above for analytics and advertising (which may qualify as “sharing” under California law).

Your Choices – Do Not Sell or Share: If you prefer that your personal information not be used for targeted advertising purposes, you have several options to opt out:

- **Global Privacy Control (GPC):** We honor GPC signals. This means if you have enabled a browser setting or extension that broadcasts the “GPC” signal, our website will treat that as a valid request to opt out of the sale/sharing of your personal information. Upon detecting GPC, we will disable third-party advertising trackers on our site for that browser or device, without further action needed from you. *(Note: Ensure the GPC signal is enabled on each browser you use. We currently do not respond to the older “Do Not Track” header, which is different and not widely standardized.)*

- **“Do Not Sell or Share My Personal Information” Link:** You can directly opt out by clicking the “Do Not Sell or Share My Personal Information” link on our website (typically found in the footer or in our privacy preference center). By doing so, you instruct us to disable any data transfers that would be considered selling or sharing of your personal info. This will generally result in the same outcome as using GPC – third-party advertising cookies will be blocked or anonymized for your browser/app session.

- **Cookie Preferences:** We provide a Cookie Preferences tool on our site that allows you to manage which types of cookies are active. For example, you can choose to opt out of “Advertising Cookies” and/or “Analytics Cookies” while still allowing essential cookies. You can adjust these settings at any time by revisiting the Cookie Preferences link. Note that essential cookies (for core functionality) cannot be disabled as they are necessary for the service to work. If you use our mobile app, your device settings may allow you to limit tracking (for instance, selecting “Limit Ad Tracking” on iOS or “Opt out of Ads Personalization” on Android). Our app will respect those device-level preferences for advertising.

- **Limit Use of Sensitive Personal Information:** While we do not use sensitive personal information (SPI) for purposes that would trigger the CPRA “Limit Use of SPI” right (we only use sensitive data to provide the services you request), we still provide a “Limit the Use of My Sensitive Personal Information” option in our privacy settings. By activating this, you can further ensure that we do not use or disclose any sensitive data (such as health or precise location) beyond what is necessary for the core services. If you submit this request, we will treat it as an extra layer of opt-out/consent withdrawal for any secondary uses of sensitive info. *(As noted, our default practice is already to refrain from such secondary uses.)*

- **Analytics Opt-Out:** For Google Analytics specifically, Google provides a browser add-on to opt out of data collection (available on Google's site). You may also opt out of interest-based Google ads by adjusting your Google Ads settings. For Facebook/Meta, you can adjust your ad preferences in your Facebook account. Note that these are platform-specific controls. Using our Privacy Preferences center may be a more straightforward way to cover all third-party trackers on our site with one action.

- **"Do Not Track" Signals:** As mentioned, we do not respond to "Do Not Track" (DNT) HTTP headers at this time. DNT is an older standard that has not been consistently adopted. Instead, we support the more robust mechanisms described above (GPC, opt-out links, cookie settings) to allow you control over data sharing.

Impact of Opting Out: If you opt out of advertising cookies and sharing, you will still see advertisements, but they will likely be less relevant to you and not based on your interactions with our services. Opting out of analytics cookies may limit our ability to understand usage patterns, but our site/app should still function for you. We do not retaliate or deny service for exercising these choices (see Section 9 on Non-Discrimination), though some functionality that relies on those tools might be degraded (for example, if you block all cookies, certain preferences might not be saved, or our web chat support might not remember you between visits).

For more information or assistance with managing your tracking preferences, please contact us at **support@aspect-health.com**.

8. How We Disclose Personal Information

We do not disclose (share or sell) your personal information to unrelated third parties for their own independent use, except as described in this Policy or with your consent. When we do disclose personal information, it is primarily to service providers or contractors who act on our behalf, or in some cases to other entities that may act as independent controllers for limited purposes (for example, partners involved in advertising or if you direct us to share data with your doctor). This section outlines to whom and under what circumstances we disclose personal information.

Disclosure to Service Providers / Processors: We share personal information with trusted third-party companies and individuals who provide services to us and process data on our instruction (commonly known as "service providers" under U.S. law, or "processors" under GDPR). These service providers are bound by contractual obligations to keep personal information confidential and to use it only for the purposes of providing their services to us (not for their own purposes). Key categories of service providers we use include:

- **Cloud Hosting and Infrastructure:** e.g. Amazon Web Services (AWS), Google Cloud Platform – these services host our databases, application servers, and files, enabling us

to store and transmit data securely and reliably.

- **Data Analytics and Usage Monitoring:** e.g. Amplitude (product analytics), Google Analytics/Firebase (user behavior analytics), Crashlytics or Sentry (crash reporting). These tools help us analyze how the app or site is used and improve stability. They may collect device identifiers, usage events, and technical info on our behalf. We configure these providers to limit data use (for instance, IP anonymization where available), and they are not allowed to use the data for any purpose other than providing services to us.

- **Payment Processors:** e.g. Stripe (for handling credit card transactions). When you make payments, your payment information is sent directly to our payment processor, which processes the payment and notifies us of the result. These processors are PCI-DSS compliant and authorized to use your payment data only to process transactions and related compliance (like fraud screening). We do not see or store your full card number.

- **Email, Text Messaging, and Communications:** e.g. SendGrid or Mailchimp for sending emails; Twilio for sending text messages or phone calls; Intercom or Zendesk for managing customer support inquiries and in-app chat. These services help us communicate with you efficiently. They process your contact info and message content under our instructions.

- **Artificial Intelligence and Transcription Services:** If we use any third-party service to assist with AI note-taking or speech-to-text transcription (for instance, an AI API for converting audio to text), those third parties act as processors, meaning they cannot use your session data for anything other than providing the transcription or AI service to us. We ensure any such provider is reputable and has strong privacy commitments (for example, they do not retain or train on your data unless explicitly authorized, and we would opt out of any such retention). Whenever feasible, we use in-house or self-hosted AI models to avoid external disclosure of sensitive content.

- **Business Operations Tools:** We rely on various other operational support services. For example, database backup services; cybersecurity vendors (to detect intrusions or threats); content delivery networks (to efficiently deliver our app/website globally); and general IT and office software. These providers might incidentally process personal data, but only to the extent needed to perform their functions, and they are not permitted to use it for independent purposes.

- **Professional Advisors:** We may share information as needed with our attorneys, accountants, auditors, or insurers in the course of receiving their services. For instance, if we face a legal claim, our attorneys may need to review relevant user data to advise us. These parties are generally bound by confidentiality or legal privilege obligations.

When we disclose information to service providers, we minimize the data shared to what is necessary for them to perform their function. For example, our email provider has your email address and name to send emails, but not your health data; our hosting provider stores data but generally does not access content unless needed for troubleshooting under our direction. We also require that our service providers implement strong security measures to protect your data and agree to privacy terms that align with our standards.

Disclosure to Third Parties as Independent Controllers: In certain circumstances, we may disclose personal information to third parties that are not acting purely on our instructions, but rather determine their own purposes for processing the data. In these cases, the third party is an independent controller of the data (or in California terms, simply a "third party"), and the use of data by that party is governed by their privacy policies. Such disclosures are limited and generally fall into the following scenarios:

- **Advertising and Analytics Partners:** As discussed in Section 7, when we allow third-party advertising or analytics cookies on our site, those third parties (like Google or Meta/Facebook) collect personal information (device identifiers, browsing information) for their own analytics or advertising purposes. We do not directly hand them your account data, but by integrating their technologies, certain information is automatically transmitted to them. They act as independent controllers of that data (for example, Google might use it to improve their analytics services, or Meta might use it to personalize ads beyond our campaigns). We contractually and through settings attempt to limit the scope of data they collect (for instance, by using Google Analytics in a mode that restricts data use), but these partners ultimately determine how to use the data in line with their own user agreements and privacy policies. You have rights to opt out of this kind of sharing as detailed in Section 7.

- **Integration or Data Transfer at Your Direction:** We will share your personal information with a third party if you specifically request or direct us to do so. For example, if in the future we enable a feature where you ask us to share your wellness report with your personal doctor, or to import/export data to a third-party health app, we will do so with your authorization. Similarly, if you engage with Aspect on social media (e.g. tagging us in a post, or clicking a "share" button in our app), your information may be shared with that platform based on your action, and that platform's privacy policy will apply to the information provided.

- **Corporate Transactions:** If we undergo a business transaction such as a merger, acquisition by another company, reorganization, or sale of some or all assets, personal information may be disclosed to the acquiring or merging entity and its advisors as part of due diligence and transferred as part of the business assets. In such events, we will ensure that any successor entity honors the commitments in this Privacy Policy or provides notice and obtains consent if they plan to use personal information in a materially different way.

- **Legal Requirements and Protection of Rights:** We may disclose personal information to third parties (such as courts, law enforcement agencies, regulators, or opposing litigants) if we believe disclosure is required to comply with a law, regulation, legal process, or governmental request. We may also disclose information to enforce or apply our Terms of Service or other agreements, or to protect the rights, property, or safety of Aspect, our employees, our users, or others. This could include exchanging information with other companies and organizations for fraud prevention or investigating security incidents. Such disclosures will be made only to the extent permitted or required by applicable law. (For example, if we receive a subpoena for session records, we would only produce them if legally compelled after verifying its validity and, when possible, giving you notice.)

- **Affiliates:** Aspect Health Global Inc. currently operates as a single company. If in the future we have subsidiaries, parent, or affiliated companies, we may share personal information within our corporate family in order to provide consistent service and operations. For instance, if Aspect expands internationally and sets up a local subsidiary, data may be shared with that entity. Any such affiliate would uphold the same privacy protections described in this Policy.

- **Public and De-Identified Information:** We may share aggregated or de-identified information publicly or with third parties for various purposes. For instance, we might publish a report on overall Program outcomes (e.g., “70% of our participants saw reduced glucose variability after 3 months”) or collaborate with researchers using datasets that do not contain personal identifiers. Such information cannot reasonably be linked back to you, so it is not considered personal information.

Common Third Parties We Work With: To give you more transparency, here is a non-exhaustive list of external services we may use and that could receive personal information in one of the ways described above:

- **Amazon Web Services (AWS)** – cloud hosting and infrastructure (service provider)

- **Google Cloud / Firebase / Google Analytics** – cloud hosting and analytics tools (service provider for hosting; independent third party for some analytics as described)

- **Stripe** – payment processing platform (service provider)

- **Intercom / Zendesk** – customer support and messaging platforms (service providers)

- **Twilio** – SMS, voice call and authentication services (service provider)

- **SendGrid** – email delivery service (service provider)

- **Meta (Facebook)** – advertising platform (third party for ads, via tools like Facebook Pixel)

- **Google Ads** – advertising platform (third party for ads)

- **Apple HealthKit / Google Fit** – user-directed data integration platforms (they act as controllers of their data, sharing with us upon your request)

- **OpenAI (or similar AI services)** – (if used for AI processing; they would act as processors under our instructions. *As of now, our AI note feature is primarily in-house.*)

We will update this Policy or provide notice if we significantly expand our sharing of personal information to additional third parties not covered above.

No Unauthorized Third-Party Marketing: We do not rent or sell your personal details to data brokers or unrelated third-party marketers. We also do not share your information with third parties for their direct marketing purposes unless you have a relationship with that third party and you explicitly direct or consent to such sharing. (For example, if an employer or insurance company sponsors your participation in the Program, and with your agreement, we might share high-level progress information with them — but such cases would be clearly explained to you in context and handled in compliance with privacy laws.)

If you have any questions about third parties that may have access to your information, you can contact us at **support@aspect-health.com**, and we will be happy to provide you with further detail.

9. Your U.S. State Privacy Rights

Depending on where you live, you may have certain privacy rights regarding your personal information. Aspect is committed to respecting those rights and providing all our users – especially residents of California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Delaware, and New Jersey – with control over their data as required by law. This section describes the rights that consumers in these states (and in some cases others) have, and how you can exercise them. We also extend many of these rights to **all** our users (even if not strictly required), as part of our commitment to privacy transparency.

Right to Know / Access: You have the right to request that we disclose what personal information we have collected about you. In response to a verified request, we will provide: (a) the categories of personal information we have collected; (b) the specific pieces of personal information we hold about you; (c) the categories of sources from which the information was collected; (d) the business or commercial purposes for collecting, using, or disclosing the information; and (e) the categories of third parties to whom we have disclosed your information (including whether any were “sold” or “shared,” which, as noted, we do not do except for the

limited sharing described). You may request a copy of the specific personal data we have about you in a readily usable format that allows you to transmit it to another entity (this is often called the right to data portability).

Right to Delete: You have the right to request deletion of personal information we have collected from you and retained, subject to certain exceptions. Once we receive and confirm a verifiable deletion request, we will delete (and direct our service providers/contractors to delete) your personal information from our records, unless an exception applies. Please note that we may deny deletion requests if retaining the information is necessary for us or our service providers to, for example: complete a transaction or service you requested; detect security incidents or protect against malicious activity; exercise or defend legal claims; comply with a legal obligation; or for certain internal purposes compatible with the context of your relationship with us. We will inform you of any specific exception that applies to a denied request.

Right to Correct: You have the right to request that we correct inaccuracies in your personal information, taking into account the nature of the information and purpose of processing. If you believe any information we maintain about you is incorrect or outdated (for example, your contact information or certain health metrics), you may request a correction. We may need to verify the accuracy of the new information you provide, and we will correct our records if appropriate. In some cases, if we cannot verify the information you've provided, we might delete the contested data or note it as disputed rather than maintain inaccurate records.

Right to Opt Out of "Sale" or "Sharing" (Targeted Advertising): You have the right to direct us not to sell your personal information to third parties, and to opt out of any sharing of your personal information for cross-context behavioral advertising (i.e. targeted ads). As explained, Aspect does **not** sell personal info for money, but we do share certain data with third-party advertising and analytics partners (see Sections 7 and 8). You can exercise this opt-out right by using the methods described in Section 7 (for example, the "Do Not Sell or Share" link or GPC signal, etc.) or by contacting us with your opt-out request. Once you opt out, we will cease any such sharing of your data for targeted advertising from that browser/device or account, as applicable. If you later consent (for example, by toggling cookie preferences back on), we will treat that as a new permission until you opt out again.

Right to Limit Use of Sensitive Personal Information: California residents have the right to request that we limit our use or disclosure of Sensitive Personal Information (SPI) to the purposes authorized by law. Other states (like Colorado, Virginia, etc.) require opt-in consent for processing sensitive data, which we have obtained from you for your health information through your Program enrollment. Aspect already restricts sensitive data (like health, biometrics, or precise location) to only necessary uses, as outlined in this Policy. We do not use SPI to infer characteristics about you, nor for third-party marketing. Nonetheless, if you are a California resident (or any user) who prefers to ensure no secondary use of your sensitive data, you may submit a "Limit SPI" request via our website or by contacting us. We will honor such requests by not using or disclosing your sensitive data beyond what is needed to provide our services or as otherwise permitted by law (such as for security, short-term system functionality, or non-personalized advertising).

Right to Opt Out of Profiling / Automated Decisions: Residents of Colorado, Virginia, and certain other states have the right to opt out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Aspect **does not** engage in any such automated decision-making without human involvement. We do not make decisions that affect your legal rights or similarly significant rights (like eligibility for services, credit, employment, etc.) based solely on automated processing of personal data. Any analysis or "profiling" we do (for example, categorizing your wellness progress) does not result in decisions that negatively affect you without human review. If this practice changes in the future, we will update this Policy and provide an opt-out mechanism. You may inquire for more information if needed.

Right of Non-Discrimination: We will not discriminate against you for exercising any of your privacy rights. This means we will not deny you our services, charge you a different price, or provide a lesser quality of service just because you exercised your rights under these laws. (However, please note that if you request deletion of certain data, it may affect our ability to provide some aspects of the Program — for example, if you delete all health data, the coaching experience may be limited. In such cases, we will explain the impact and try to find an alternative solution rather than simply denying service.) We do not offer financial incentives for your data, so there is no differential treatment to disclose.

Right to Appeal: If for any reason we are unable to fulfill your request and we deny or partially deny it (for example, we cannot verify your identity, or an exception applies that prevents deletion), you have the right to appeal our decision. To appeal, you may reply to our response indicating you would like an appeal, or send a new request to **support@aspect-health.com** with the subject "Privacy Request Appeal," including the details of your original request and our response. A different, senior reviewer will examine your appeal and we will respond with the outcome within the time frame required by law (generally 45 days). If we deny your appeal, we will provide an explanation. For Virginia, Colorado, and other applicable state residents, if you are not satisfied with the outcome of the appeal, you may contact your state's Attorney General or data protection authority to lodge a complaint. We will provide those instructions in our appeal response if applicable.

Exercising Your Rights: To exercise any of the rights above, please submit a request to us by one of the following methods:

- **Email:** Send an email to **support@aspect-health.com** with the subject line "Privacy Rights Request." In the email, let us know which right(s) you wish to exercise (e.g. access, deletion, correction, opt-out) and provide sufficient information for us to verify your identity and process the request (such as your name, email, and details about your request).

- **Online Form:** If available, you may use our online Privacy Request form (accessible through our website's Privacy Center or footer link). This form will ask for the necessary details to process your request.

- **Phone:** At this time we do not have a dedicated toll-free number for privacy requests. If this changes, we will update this Policy. For now, email is the most efficient method.

We may need to verify your identity before processing your request, to ensure that the person making the request is actually you (or your authorized agent). For verification, if you have an account, we may ask you to submit the request through your logged-in account or to confirm information through a code sent to your email. If you do not have an account or cannot access it, we might ask you to provide a few pieces of information that we can match against our records (such as a recent transaction amount, date of last interaction, or other details we have on file). For requests involving highly sensitive information (like access to health data or deletion of extensive records), we may require a higher level of verification (for example, multiple data points or a signed declaration) consistent with legal requirements. If we cannot verify your identity to a sufficient degree of certainty, we will inform you and may have to deny the request for safety reasons, but you can provide additional information or try again.

Authorized Agents: You may designate an authorized agent to make a request on your behalf (for California residents and perhaps others). If you do so, we will take steps to verify the agent's authority and your identity. For example, if an agent (such as an attorney or a family member) submits a request on your behalf, they should provide a signed written permission from you or proof of power of attorney. We may also contact you directly to confirm the agent's authority. The exact verification requirements will depend on the sensitivity of the request. If an agent fails to provide proof of authorization, we will deny the request.

Response Timing: We will confirm receipt of your request within 10 days (for California residents) and provide information on how we will process it. We strive to respond to all verifiable consumer requests within 45 days of receipt. If we need more time (up to an additional 45 days, for a total of 90 days), we will inform you of the reason and extension in writing within the initial 45-day period. If you have an account with us, we will deliver our written response to the email associated with your account (or via your account interface if appropriate). If you do not have an account, we will send it to the contact information provided (usually email, or postal mail if you request and provide a mailing address).

Our response will explain the actions we took (or did not take) and the reasons. For access requests, we will either provide the requested information or explain why we cannot (if an exception applies). For deletion requests, we will confirm that we deleted your information or, if we must retain certain pieces, we will inform you of the reason. For correction, we'll confirm the data is corrected or explain if we cannot make the change. Any disclosures we provide will typically cover the 12-month period preceding the receipt of your request, unless you request a longer timeframe and the law allows it (California allows requesting information beyond 12 months in certain cases, subject to feasibility). We do not charge a fee for processing your request unless it is excessive, repetitive, or manifestly unfounded. If we determine a fee is warranted, we will explain why and provide a cost estimate, giving you the option to proceed or withdraw your request.

We value your privacy rights and will do our best to honor them in accordance with the law. If you have any questions about your rights or need assistance, please contact us at **support@aspect-health.com**.

10. Data Retention

We retain personal information only for as long as reasonably necessary to fulfill the purposes for which it was collected, as described in this Policy, or as required by law. Specific retention periods for different categories of data were outlined in the Notice at Collection table (Section 3). Below is a summary of our retention practices:

- **Account and Contact Data:** We keep basic account information (like your name, contact details, login credentials) for as long as you have an active account. If you terminate your account or your Program ends, we will delete or anonymize this information within a set period (generally within 30–90 days after account closure), except where we need to retain it for legitimate business or legal reasons. For instance, we may retain certain contact or transaction details for a longer period to handle refunds, disputes, or to comply with financial recordkeeping laws. Typically, we retain basic account and transaction records for up to 3 years post-account deletion, unless a longer retention (e.g. 7 years for payment records to meet tax and accounting requirements) is required.

- **Health and Wellness Data:** We maintain your health, wellness, and CGM data for as long as you are actively participating in the Program, so that you (and we) have access to your historical trends and progress. After you leave the Program or if you request deletion, we will delete or de-identify this data after a short grace period (approximately 90 days), unless we have a specific reason to keep it. Specific reasons might include an unresolved issue or inquiry requiring the data, the need to defend against legal claims involving the data, or an explicit legal requirement to retain it. In the absence of these, we prefer not to hold sensitive data longer than necessary. When deleting, we scrub it from active databases and request the same of our service providers. (Backup copies might persist for a short time until they are overwritten according to our backup retention schedule.)

- **Session Recordings:** As noted, raw coaching session recordings and transcripts are kept for up to 1 year by default. In practice, many recordings (especially older ones beyond a few months) may be purged earlier once they've served their purpose. AI-generated summaries might be kept slightly longer than the raw audio/video, but only in a form that is not directly identifying, and solely for internal reference or to improve our services. If you withdraw consent for recordings, any existing identifiable recordings will be deleted (or fully anonymized) within roughly 30 days of your request, barring any legal need to retain them.

- **Usage Logs and Analytics:** We generally retain server logs and detailed usage data for about 12 months. Aggregated analytics (which contain no personal identifiers) may be stored indefinitely for trend analysis. Certain high-level usage metrics might be kept longer to understand historical performance, but these wouldn't identify individual users. Shorter retention may apply to some specific logs (e.g. security logs might only keep 90 days of data unless flagged for investigation). Advertising-related data (like cookie identifiers) is often governed by the lifespan of the cookie (often 6–24 months) or your opt-out status (if you opt out, we stop retaining new advertising identifiers).

- **Communications:** Emails and customer support correspondence are usually kept for up to 2 years, which helps us have context if you contact us again or to improve our support processes. Call recordings (for support calls) are typically kept for about 90 days unless we need to retain them longer for training or to resolve a specific issue. If a particular support interaction results in a legal matter, relevant communications might be retained until that matter is resolved and then deleted according to our standard schedule.

- **Legal Hold:** If any information is subject to a legal hold (for example, because of litigation or a government investigation), we will retain that information until the hold is lifted, even if it surpasses the normal retention period. We also may retain information as needed to comply with court orders or settlements.

After the applicable retention period ends, we will take steps to permanently delete, destroy, or de-identify the personal information. De-identification means altering or removing identifying details so that the data can no longer reasonably be linked to you. We may retain de-identified data (which is not considered personal information) for research or statistical purposes without further notice to you.

Please note that residual copies of data might remain in our system backups for a short duration beyond the active deletion timeline, but such backups are protected and eventually cycle out as new backups overwrite them. We maintain backup data purely for disaster recovery and continuity purposes; it is not readily accessible for routine business use and is governed by strict retention and security protocols.

If you have specific questions about our data retention practices for any particular type of data, you can contact us for more details. We can also, upon request, consider any reasonable adjustments to our retention policies in particular circumstances (for example, if you have a compelling need for us to delete certain data sooner, we will try to accommodate it if legally and operationally feasible).

11. Data Security

We understand the importance of securing your personal information. Aspect has implemented a comprehensive array of technical, administrative, and physical security measures designed to

protect your data against unauthorized access, disclosure, or destruction. However, no method of transmission over the internet or electronic storage is 100% secure, so we cannot guarantee absolute security. We want to be transparent about how we strive to protect your information:

- **Encryption in Transit and at Rest:** All personal information transmitted through our app or website is protected using encryption (TLS/HTTPS) in transit. This means data exchanged between your device and our servers is encrypted to prevent eavesdropping. Additionally, we encrypt sensitive personal data at rest in our databases and storage systems. For example, health records, session recordings, and passwords (hashed and salted) are secured using strong encryption algorithms.

- **Access Controls and Authentication:** Access to personal information within Aspect is restricted to authorized employees or contractors who have a legitimate need to know that information to perform their job duties. We employ role-based access controls so that each individual only has the minimum access necessary. All personnel with such access must authenticate using strong credentials, and multi-factor authentication is enforced for administrative access. We regularly review access privileges and revoke accounts or permissions that are no longer needed.

- **Network and Application Security:** We use industry-standard security tools and practices to safeguard our systems. This includes firewalls to protect our network, intrusion detection and prevention systems, and continuous monitoring of our infrastructure for suspicious activities. We apply security patches and updates to our software and systems in a timely manner to address vulnerabilities. Our application undergoes periodic security assessments, including vulnerability scanning and penetration testing by independent experts, to identify and fix potential weaknesses.

- **Data Pseudonymization:** Where feasible, we separate direct identifiers from more sensitive data. For example, we might store your personal identifiers (like name or contact info) in a different database from your health and wellness data, using an internal user ID to link them. This means that even if one dataset were compromised, it would not easily reveal your identity without the linking key. We also use pseudonymous identifiers in certain analytics (e.g. random device IDs or hashed tokens) rather than real names or emails.

- **Employee Training and Policies:** All staff and contractors are trained on data privacy and security best practices, including how to handle sensitive information and recognize potential security threats like phishing attempts. We have internal policies (and, where appropriate, confidentiality agreements) that obligate our team to protect your information and maintain confidentiality. Employees are instructed to adhere to the principle of least privilege and to report any potential security incidents immediately.

- **Vendor Due Diligence:** When we engage third-party service providers who may process personal data (as listed in Section 8), we conduct diligence on their security

practices. We choose reputable providers with strong security track records and require them to commit contractually to protecting personal information with standards equal to or greater than our own. We also include data protection agreements or clauses (such as Standard Contractual Clauses for international transfers, discussed below) as needed.

- **Anonymization and Data Minimization:** We strive to collect only the personal information that we need for the stated purposes. If data is no longer needed in identifiable form, we will anonymize or aggregate it. For example, we may retain wellness trend data in an aggregated format (without personal identifiers) for research, rather than keeping the raw personal data indefinitely. By minimizing what we retain, we reduce the risk in case of any unauthorized access.

- **Physical Security:** The personal information we handle is stored in secure data centers with robust physical security controls (such as gated entrances, security personnel, surveillance cameras, and access badge requirements). Within our own offices, any physical documents containing personal data (which is rare, since our operations are mostly digital) are kept in locked cabinets and shredded or securely destroyed when no longer needed.

- **Incident Response:** We maintain an incident response plan to handle any suspected data security incident swiftly and effectively. This plan includes steps for investigation, containment, eradication of the threat, recovery of systems, and notification of affected parties and authorities as required. In the unlikely event of a data breach that compromises personal information, we will notify affected individuals and any relevant regulatory bodies in accordance with applicable breach notification laws.

- **No Absolute Guarantee:** While we are committed to protecting your data, we must emphasize that no security measure or system is infallible. There is always a possibility of unforeseen events or sophisticated attacks that could lead to a security breach. We continuously update and adapt our security measures to new threats and strive to meet or exceed industry standards, but we cannot promise that personal information will remain absolutely secure in all circumstances.

- **Your Responsibility:** You also play a vital role in keeping your personal information secure. We encourage you to use a strong, unique password for your account and to keep it confidential. Do not share your account credentials or verification codes with others. Be cautious of “phishing” attempts — Aspect will never ask you for your password or sensitive information via unsolicited communications. Always ensure that communications you receive claiming to be from us are legitimate (e.g., check the email domain). If you suspect any unauthorized access to your account or personal data, please notify us immediately at **support@aspect-health.com** so we can assist in securing your account.

By using our services, you acknowledge that you understand the measures we take to protect your data and their inherent limitations. We will continue to invest in security to earn and maintain your trust.

12. International Data Transfers

Aspect Health Global Inc. is based in the United States, and our Program is primarily designed for U.S. users. If you are accessing our services from outside the United States, please be aware that your personal information will likely be transferred to, stored, and processed in the United States (or other jurisdictions where our service providers operate, such as Canada or the European Union). The data protection laws in these countries may be different from, and less protective than, the laws of your country of residence. However, regardless of where your data is processed, we will handle it in accordance with this Privacy Policy and will put in place appropriate safeguards to protect it.

EEA/UK Users: While our services are not specifically targeted at the European Economic Area (EEA) or the UK, it is possible that some users from these regions may use our site or Program (for example, out of interest or while traveling). If European or UK data protection law (GDPR/UK GDPR) applies to the data we collect from you, then we ensure that we have a lawful basis for processing (such as your consent, the performance of a contract with you, or our legitimate interests as described in Section 4, balanced against your rights). Additionally, if we transfer your personal data out of the EEA or UK to the U.S. or other countries not deemed "adequate" by European/UK authorities, we rely on approved transfer mechanisms to safeguard your information. These may include **Standard Contractual Clauses (SCCs)** approved by the European Commission and UK, which are contractual commitments that bind us and the recipient to protect your data to EU/UK standards. In some cases, we may rely on your explicit consent for a transfer or other exemptions allowed by law (for instance, if a transfer is necessary to perform a contract with you).

By using our service or providing us with your information, you acknowledge that your information will be transferred to and processed in the United States and potentially other jurisdictions as explained. For residents of countries with data transfer restrictions, we take steps to validate that any such transfer is done lawfully and securely. If you require more information about our international transfer practices or the specific safeguards in place, you can contact us (see Section 15).

Privacy Shield and New Frameworks: (Note: The EU-U.S. Privacy Shield framework was invalidated in 2020, so we do not rely on it for data transfers.) We are aware of the new EU-U.S. Data Privacy Framework approved in 2023 and are evaluating participation in it. Should we certify under that framework or any other officially recognized mechanism for EU-to-US data transfer, we will update this Policy accordingly. In the meantime, we continue to use SCCs and other measures for compliance.

Storage Locations: Currently, our primary data storage and processing facilities are in the United States. In certain cases, specific subsets of data might be processed or stored outside the U.S. (for example, if we use a European data center for a particular service at a user's request, or if one of our service providers uses a global content delivery network that caches data in servers closer to you for speed). However, our core databases are U.S.-based. We ensure that any transfers to or access from other countries are protected by proper safeguards as mentioned.

Your International Rights: If you are an EU/UK user, in addition to the rights described in Section 9, you have the right to lodge a complaint with a supervisory authority (such as the Data Protection Authority in your EU country, or the UK Information Commissioner's Office) if you believe we have violated your data protection rights. We do ask that you kindly attempt to resolve any concerns with us first, as we are committed to addressing your privacy questions and issues.

We will update this section as global data protection requirements evolve, and will inform you of any significant changes in how we handle international data transfers.

13. Children's Privacy & Eligibility Requirements

Our services are not intended for anyone under the age of 18. We do not knowingly solicit or collect personal information from children (minors) under 18 years old. **If you are under 18, please do not use the Program or send us any information about yourself.** If we learn that we have inadvertently collected personal information from an individual under 18, we will take prompt steps to delete such information from our records and terminate the minor's account.

Eligibility Criteria: In addition to the minimum age requirement, the Aspect Wellness Program has specific eligibility criteria to ensure user safety. We do not permit participation by individuals who fall into certain health-related categories, including but not limited to:

- **Insulin-Dependent Individuals:** Anyone currently prescribed or using insulin therapy (e.g. individuals with Type 1 diabetes or insulin-requiring Type 2 diabetes) is excluded. This is because our non-clinical program is not equipped to manage the medical risks associated with insulin use.

- **Dialysis Patients:** Individuals undergoing kidney dialysis are not eligible to participate.

- **History of Severe Hypoglycemia Unawareness:** Individuals who have a history of serious hypoglycemia episodes or an inability to detect severe hypoglycemia are excluded for safety reasons.

- **Pregnant Individuals:** The Program is not designed for those who are pregnant. Pregnancy involves unique health considerations that go beyond our wellness scope.

- **Other Medical Conditions:** There may be additional medical conditions or situations (such as certain heart conditions, eating disorders, or other conditions deemed high-risk) that we identify as contraindications to participation. These would be communicated during the enrollment screening process.

When you sign up, we ask you to confirm that you do not fall into any of the above categories. It is crucial that you answer these eligibility questions truthfully for your own safety. If your status changes **after** enrollment – for example, if you become pregnant, begin using insulin, or develop a condition mentioned above – you agree to notify us (Aspect) immediately. We will then reevaluate your participation and may advise you to pause or discontinue the Program. This is solely to ensure your well-being; in such cases we might recommend that you seek more appropriate medical supervision.

Account Termination for Ineligibility: If we discover that a participant is under 18 or otherwise ineligible (per the criteria above), we will take steps to terminate their access to the Program. For a minor, this includes deletion of all personal information collected from that individual as quickly as possible. For other ineligible cases (e.g. someone inadvertently or intentionally enrolled despite an excluded condition), we will reach out to discuss the situation. Our likely course of action will be to end the service for that individual and, where appropriate, remove their data from our active systems. We may retain minimal information necessary to document the reason for termination (for example, a record that an individual was excluded due to a medical condition) or to process a refund, but such information will be handled in compliance with privacy laws and only retained as long as necessary.

No Services to Children: We do not market or provide any services to children. By using the Program, you represent that you are at least 18 and meet the eligibility requirements. We may employ verification steps (for example, asking for identification or using third-party age verification) if we suspect a user is underage or has misrepresented their eligibility. If a parent or guardian becomes aware that their child under 18 has provided us with personal information, they should contact us at **support@aspect-health.com**. We will delete the information and close the account promptly.

While we recognize that teenagers and children could benefit from wellness guidance, our Program is not designed or licensed for that population. We encourage parents or guardians to seek appropriate services for minors through pediatric healthcare providers or programs specifically tailored for children's health. Our exclusion of minors and certain individuals is not intended as discrimination, but as a necessary measure to ensure we operate within our non-clinical scope and do not inadvertently put vulnerable individuals at risk.

If you have questions about eligibility or think you might be on the borderline of any criteria, please reach out to us **before** enrolling. We appreciate your understanding and cooperation in keeping our community safe and appropriate for the intended users.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. When we make changes, we will notify users in a manner appropriate to the significance of the changes:

Effective Date: At the top of this Policy, we list the effective date. Any changes will be indicated by updating that date. We encourage you to review this Policy periodically to stay informed about how we are protecting your information.

Notice of Material Changes: If we make any *material* changes to this Policy (especially changes that expand how we use or share personal information, or that affect your rights), we will provide a prominent notice. This may include sending an email to the address associated with your account, placing a notice on our website or within our app, or similar measures. The notice will explain the key changes and direct you to the updated Policy. For example, if we were to begin collecting new types of personal data or using existing data for new purposes not previously disclosed, that would likely be considered material and we would inform you in advance.

Consent for Certain Changes: In cases where a change involves using your personal information in a manner materially different from what was stated at the time of collection, or if required by applicable law, we will obtain your consent before applying the change to your information. For instance, if in the future we wanted to share your health data with a research partner in identifiable form (a hypothetical scenario), we would first seek your explicit permission even if our Privacy Policy is updated to describe that practice.

Administrative or Minor Changes: Non-material updates (such as clarifications, corrections of typographical errors, reorganization of content, or changes to reflect new features that do not affect privacy in a significant way) may be made to this Policy and posted without advance notice, but the effective date will still be updated to let you know a revision occurred. We consider these types of changes to be improvements in understanding or accuracy that do not negatively impact your privacy rights.

If you continue to use our services after a Policy update takes effect, your use will be deemed acceptance of the revised Policy (except in scenarios where your explicit consent is required, as noted above). However, if any change is unacceptable to you, you have the right to stop using our services and, if you wish, delete your account or exercise your data rights (such as requesting deletion of your information). We will not enforce any material changes retroactively without your consent.

We will keep prior versions of this Privacy Policy available upon request so that you can see how our practices have evolved. If you have any questions about changes to the Policy, you can always contact us for more information (see Section 15 below).

15. Contact Us

If you have any questions, concerns, or comments about this Privacy Policy or our privacy practices, or if you wish to exercise your rights and choices as described above, please contact us as follows:

Aspect Health Global Inc.
919 North Market Street, Suite 950
Wilmington, DE 19801, USA

Email: support@aspect-health.com

We will endeavor to respond to your inquiry within a reasonable timeframe. For requests involving privacy rights, as noted, we may need to verify your identity and request additional information to ensure we handle your data appropriately and securely. We appreciate the opportunity to address your questions and ensure you are satisfied with how we handle your personal information.

If you need to contact our Data Protection Officer (if one is appointed in the future) or an equivalent privacy contact, please indicate that in your communication and we will route your inquiry appropriately. For users in the EEA or UK (if applicable), you may also reach out to us at the above email for any GDPR-related concerns. While we do not currently have an EU representative (since we do not actively target the EU), we are still committed to addressing any cross-border privacy inquiries in good faith.

Thank you for trusting Aspect Health with your personal information. We value your privacy and are here to help if you have any questions or issues.

16. Definitions and Legal References

For clarity, here are some key definitions and references to laws that are relevant to this Privacy Policy:

- **“Personal Information” / “Personal Data”:** Any information that identifies, relates to, describes, or can reasonably be linked to an identifiable individual. This includes obvious identifiers like name and email, as well as less direct information like device ID, IP address, or combinations of data that can be used to identify you. “Personal Information” is a term used in U.S. privacy laws (like CPRA), while “Personal Data” is used in GDPR — for our purposes, we treat them equivalently. Personal information does **not** include de-identified data, aggregated information, or publicly available information (each as defined under applicable law).

- **“Sensitive Personal Information” (SPI):** A subset of personal information that is given extra protections under certain laws. Under the CPRA (California), this includes data like

Social Security number, driver's license or passport numbers, financial account login credentials, precise geolocation, contents of certain private communications (mail, email, texts when not intended for us), genetic data, biometric identifiers, and information concerning health, sex life, or sexual orientation. Under GDPR (referred to as "Special Categories of Personal Data"), it includes data about health, genetic or biometric data for identification, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and so on. In our context, health and CGM data would be considered sensitive personal information. We handle such data with heightened care and only use it for necessary purposes as described in this Policy.

- **"Processing":** Any operation performed on personal data, whether or not by automated means. This includes collection, use, storage, analysis, sharing, and deletion of personal data. Essentially, if we do anything with your personal information, that's processing.

- **"Controller":** The entity that determines the purposes and means of processing personal data. Aspect (the company) is the controller of the personal information collected in connection with the Program – we decide how and why the data is used (in line with what we describe in this Policy). In some jurisdictions, the term "Business" (as in CCPA/CPRA) is used similarly to indicate the primary organization responsible for the data.

- **"Processor" / "Service Provider":** An entity that processes personal data on behalf of a controller/business, following its instructions. In this Policy we often use the term *service provider* (common under U.S. laws) interchangeably with processor (the GDPR term). These entities have no independent right to use the data except as needed to perform services for us. Examples: our cloud hosting provider, our payment processor – they process data for us, subject to our contracts.

- **"Third Party":** In U.S. privacy law, this generally means an entity that is not the business that collected the data and not a service provider of that business. In simpler terms, an independent entity with whom data is shared for their own purposes. For example, when we enable data collection by Facebook via their pixel on our site, Facebook is a third party (because they use the data for their own ad targeting purposes). Under GDPR, such an entity would typically be considered an independent controller when processing your data.

- **"Sell," "Sale," or "Selling":** In the context of privacy law (like the CCPA/CPRA), selling is defined broadly. It is not limited to exchanging data for money; it can include any transfer of personal information to another business or third party for valuable consideration (benefit). For instance, trading data for services or some other benefit could be considered a sale under California law. Aspect does **not** sell personal information under these definitions — we do not exchange your data for monetary or other valuable consideration.

- **“Share” or “Sharing”:** Under the CPRA, sharing refers specifically to disclosing personal information to a third party for cross-context behavioral advertising (targeted advertising) for the benefit of the business. This can occur even without money being exchanged. In our case, as described, we *share* some usage data with advertising partners to market our services (which you can opt out of). When we say we share data in everyday language in this Policy, we usually mean any disclosure — but if capitalized or used in context of CPRA, it refers to this specific definition.

- **CPRA:** The California Privacy Rights Act of 2020, which amends and expands the California Consumer Privacy Act (CCPA) of 2018. Effective January 1, 2023, CPRA gives California consumers enhanced rights and imposes additional obligations on businesses (like including retention periods and allowing opt-out of sharing, among other things). We often refer generally to “California law” or CCPA/CPRA, and we aim to comply with those requirements for all users where applicable.

- **Other U.S. State Laws:** We also refer to the privacy laws of Colorado (Colorado Privacy Act, effective July 2023), Connecticut (CT Data Privacy Act, effective July 2023), Virginia (Consumer Data Protection Act, effective Jan 2023), Utah (Consumer Privacy Act, effective Dec 2023), Texas (Texas Data Privacy and Security Act, effective July 2024), Oregon (Oregon Consumer Privacy Act, effective July 2024), Montana (Montana Consumer Data Privacy Act, effective Oct 2024), Delaware (Delaware Personal Data Privacy Act, effective Jan 2025), and anticipated laws in other states like New Jersey. When we use the term “U.S. state privacy laws,” we mean these comprehensive consumer privacy statutes and any similar laws that may be enacted. We strive to meet the highest standard among these, even if not all provisions apply to us.

- **GDPR and UK GDPR:** The General Data Protection Regulation (EU) 2016/679 is the European Union’s comprehensive data protection law that took effect May 25, 2018. The UK GDPR refers to the United Kingdom’s version of GDPR (essentially the same standards, retained post-Brexit in the UK Data Protection Act 2018). These laws govern how personal data of individuals in the EU/UK can be processed, and include principles like lawfulness, transparency, purpose limitation, data minimization, etc., as well as rights similar to those described in Section 9. While our service is primarily US-focused, we aim to uphold these principles as a best practice and to be prepared should they apply.

- **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 is a U.S. federal law that, among other things, includes privacy and security rules for protecting certain health information (Protected Health Information, PHI) handled by specific entities (like healthcare providers, insurers, or their business associates). Aspect is **not** a covered entity under HIPAA, because we are not providing healthcare services or billing insurance, and the data you provide to us is not coming from a healthcare provider in a way that would make it PHI. Therefore, HIPAA regulations do not apply to the information you provide in our Program. Instead, your data is protected by other privacy laws (as described in this Policy) and by our own commitment to privacy. We mention

HIPAA to clarify this distinction – for example, CGM data we collect from you is not considered PHI under HIPAA, since it's part of a wellness service you opted into and not part of a medical record from a healthcare provider.

- **Data Subject:** A term mainly used in GDPR, referring to the individual whom personal data is about — in other words, you, as the user. You are the data subject in relation to the personal information you provide to us. U.S. laws often use the term "consumer" or just "consumer's personal information" similarly.

- **Consent:** Your freely given, specific, informed, and unambiguous agreement to the processing of your personal data. In practice, by enrolling in the Program (and for certain data uses, checking a consent box or signing our Post-Purchase Consent), you have consented to the data practices outlined. Under GDPR and some state laws, consent can be withdrawn at any time, and we make it as easy to withdraw as it was to give (for example, you can contact support to change your preferences or opt-outs at any time).

Legal References: For further context, here are some laws and regulations referenced or underlying our practices:

- *California* – California Civil Code § 1798.100 et seq. (CCPA/CPRA, the California Consumer Privacy Act as amended by the California Privacy Rights Act).

- *Colorado* – Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq.

- *Connecticut* – Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15).

- *Virginia* – Virginia Consumer Data Protection Act (Va. Code § 59.1-575 et seq.).

- *Utah* – Utah Consumer Privacy Act (2022 Utah SB 227).

- *Texas* – Texas Data Privacy and Security Act (effective July 2024).

- *Oregon* – Oregon Consumer Privacy Act (2023 OR SB 619, effective July 2024).

- *Montana* – Montana Consumer Data Privacy Act (2023 MT SB 384, effective Oct 2024).

- *Delaware* – Delaware Personal Data Privacy Act (2023 DE HB 154, effective Jan 2025).

- *New Jersey* – (Pending legislation for a New Jersey Consumer Privacy Act; we are monitoring its progress as of the effective date of this Policy.)

- *European Union* – General Data Protection Regulation (EU) 2016/679 (GDPR).

- *United Kingdom* – UK Data Protection Act 2018 and UK GDPR.

By including these references, we want to convey that we are aware of and aligning our practices with the relevant privacy laws. If you'd like further information on any of these laws or how we comply with them, feel free to contact us.

Last Updated: October 15, 2025.