

Privacy Policy

Ave Health Partners, Inc. Effective Date: July 20, 2026 Last Updated: July 20, 2026

1. Introduction

Ave Health Partners, Inc. ("**Ave Health Partners**," "**we**," "**us**," or "**our**") provides health data analysis and custom reporting services to our clients through our website and related services (collectively, the "**Services**"). This Privacy Policy explains how we collect, use, disclose, store, and protect personal information and personal health information (as defined below) in connection with the Services, and describes the rights and choices available to individuals whose information we handle.

This Privacy Policy is designed to comply with applicable federal law — including the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act ("**HIPAA/HITECH**"), and the Federal Trade Commission Act — as well as applicable North Carolina law, including the North Carolina Identity Theft Protection Act (N.C. Gen. Stat. § 75-60 et seq.) and other relevant North Carolina consumer protection statutes.

By using our website or Services, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our practices, please do not use the Services.

2. Scope and Roles

Ave Health Partners collects, processes, and stores personal information and personal health data on behalf of our clients ("**Clients**") for the purpose of performing data analysis and generating custom health reports. Depending on the nature of the engagement:

- Where Ave Health Partners creates, receives, maintains, or transmits protected health information ("**PHI**") on behalf of a Client that is a HIPAA "covered entity" (e.g., a health plan, health care provider, or health care clearinghouse), Ave Health Partners acts as a **HIPAA Business Associate**, and our handling of that PHI is additionally governed by a **Business Associate Agreement ("BAA")** executed with the applicable Client, which controls in the event of any conflict with this Policy.
- Where Ave Health Partners collects health information directly and is not acting on behalf of a HIPAA covered entity, we nonetheless apply HIPAA-equivalent administrative, physical, and technical safeguards to that data as a matter of policy and contractual commitment to our Clients.

Data Ownership. All personal information and personal health data submitted to Ave Health Partners by or on behalf of a Client remains the property of that Client (or the individual to whom the data pertains, as applicable). Ave Health Partners does not claim ownership of Client data and processes it solely to provide the Services, as further described below.

3. Information We Collect

3.1 Personal Information

We may collect the following categories of personal information from Clients, Client personnel, website visitors, and other individuals:

- Identifiers: name, email address, mailing address, phone number, employer/organization, job title
- Account credentials: usernames, passwords (stored in hashed/encrypted form)
- Billing and payment information (processed via a secure third-party payment processor)
- Communications: correspondence, support requests, and inquiries submitted to us
- Technical/usage data: IP address, browser type, device identifiers, cookies, and similar website usage data (see Section 9)

3.2 Personal Health Data

In connection with the Services, we may collect, receive, or process health-related information submitted by or on behalf of our Clients, which may include:

- Demographic and identifying health information (e.g., date of birth, sex, patient/member identifiers)
- Clinical, diagnostic, treatment, medication, laboratory, or claims data
- Health plan or insurance-related information
- Any other individually identifiable health information provided to us for the purpose of analysis and report generation

We collect this information directly from Clients (e.g., via secure upload, API integration, or file transfer) and do not independently solicit health information from individual patients or members except as directed by a Client.

4. How We Use Information

We use personal information and personal health data solely for the following purposes:

1. **Providing the Services** — performing data analysis, generating custom reports, and delivering deliverables to the Client that submitted or authorized submission of the data;
2. **Account and service administration** — creating and managing accounts, processing payments, and providing customer support;
3. **Security and integrity** — detecting, investigating, and preventing fraud, unauthorized access, and security incidents;

4. **Legal compliance** — meeting our obligations under HIPAA, North Carolina law, and other applicable law, including responding to lawful requests from regulators or courts;
5. **Service improvement** — with de-identified or aggregated data only (see Section 5), improving the accuracy, performance, and functionality of our analytics tools.

We do **not** sell personal information or personal health data. We do **not** use Client health data for marketing, advertising, or any purpose unrelated to providing the Services, except with the Client's express written authorization.

5. De-Identified and Aggregate Data

We may create de-identified or aggregated data sets from health information in accordance with HIPAA de-identification standards (45 C.F.R. § 164.514). Once information has been de-identified in accordance with these standards, it is no longer considered personal health data, and we may use it for purposes such as improving our analytical models, internal research, and service development. We will not attempt to re-identify de-identified data except as permitted by law.

6. How We Disclose Information

We disclose personal information and personal health data only as follows:

- **To the Client**, in the form of custom reports, dashboards, or analysis deliverables, as directed by the engagement;
- **To subprocessors and service providers** who perform functions on our behalf (e.g., cloud hosting, secure storage, customer support tools), each of whom is bound by written agreements — including, where applicable, a Business Associate Agreement — requiring them to protect the information consistently with this Policy and applicable law;
- **As required by law**, including in response to a valid subpoena, court order, or regulatory request, or as otherwise required under HIPAA, North Carolina law, or other applicable statutes;
- **In connection with a business transaction**, such as a merger, acquisition, financing, or sale of assets, subject to the acquiring party's agreement to honor the commitments in this Policy (and any applicable BAA);
- **With your or the Client's consent**, for any other purpose disclosed at the time of collection or separately authorized in writing.

We do not disclose personal health data to third parties for marketing purposes, and we do not permit third parties to use Client data for their own independent purposes.

7. Data Storage and Security

7.1 HIPAA-Compliant Cloud Storage

All personal health data collected or processed by Ave Health Partners is stored in a HIPAA-compliant, secure cloud database environment. Our cloud infrastructure providers execute Business Associate Agreements with us where required and maintain administrative, physical, and technical safeguards consistent with the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C), including:

- Encryption of data at rest and in transit (industry-standard encryption protocols)
- Role-based access controls and multi-factor authentication
- Audit logging and monitoring of access to health data
- Regular vulnerability assessments and security testing
- Data backup, disaster recovery, and business continuity protocols
- Employee training on HIPAA and data privacy requirements, and confidentiality/access agreements for all personnel with access to PHI

7.2 Data Minimization and Access Controls

Access to personal health data is restricted to personnel and systems that require it to perform the Services, on a least-privilege, need-to-know basis.

7.3 No Absolute Guarantee

No method of electronic storage or transmission is 100% secure. While we use commercially reasonable and industry-standard safeguards designed to protect your information, we cannot guarantee absolute security.

8. Data Retention

We retain personal information and personal health data only for as long as necessary to provide the Services, fulfill the purposes described in this Policy, and comply with our legal and contractual obligations (including HIPAA's six-year documentation retention requirement, where applicable). Retention periods for Client health data are further governed by the applicable service agreement or Business Associate Agreement. Upon termination of an engagement, and upon a Client's written request, we will return or securely destroy Client data in accordance with the terms of the governing agreement and applicable law, unless retention is required by law.

9. Cookies and Website Tracking Technologies

Our website may use cookies, web beacons, and similar technologies to operate the site, remember preferences, and analyze site usage. These technologies do not collect personal health data. You can control cookies through your browser settings; disabling cookies may affect the functionality of the website. We do not use tracking technologies to serve targeted advertising based on health information.

10. Your Rights and Choices

10.1 Individual Rights Regarding Health Information

Where Ave Health Partners maintains PHI as a Business Associate, individual requests to access, amend, or obtain an accounting of disclosures of health information should generally be directed to the applicable Client (the HIPAA covered entity), who is responsible for responding to such requests. We will assist our Clients in fulfilling these obligations as required under the applicable Business Associate Agreement and HIPAA.

10.2 General Privacy Rights

Depending on your relationship with us, you may have the right to:

- Request access to the personal information we hold about you
- Request correction of inaccurate personal information
- Request deletion of your personal information, subject to legal and contractual retention requirements
- Opt out of non-essential communications
- Withdraw previously provided consent, where processing is based on consent

To exercise these rights, please contact us using the information in Section 14. We will respond in accordance with applicable law and any applicable Client agreement.

10.3 North Carolina Residents

Under the North Carolina Identity Theft Protection Act, we maintain reasonable security procedures to protect personal information from unauthorized access and disclosure, and we will notify affected individuals and, where required, the North Carolina Attorney General, in the event of a security breach involving unencrypted personal information, in accordance with N.C. Gen. Stat. § 75-65.

11. Data Breach Notification

In the event of a breach of unsecured protected health information, Ave Health Partners will provide notification in accordance with the HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D) and, where applicable, will notify affected Clients without unreasonable delay so that Clients may fulfill their own notification obligations. For breaches involving personal information not subject to HIPAA, we will provide notification consistent with the North Carolina Identity Theft Protection Act and other applicable state breach notification laws.

12. Children's Information

Our Services are intended for use by businesses and are not directed to individuals under the age of 18. We do not knowingly collect personal information directly from children. To the extent health data

pertaining to minors is submitted by a Client in the course of the Services, it is handled with the same safeguards described in this Policy and any applicable Business Associate Agreement.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. We will post the revised Policy on our website with an updated "Last Updated" date. Material changes affecting the handling of health data will be communicated to affected Clients in accordance with any applicable service agreement or Business Associate Agreement.

14. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact:

Ave Health Partners, Inc. Attn: Privacy Officer [Street Address] [City, State ZIP] Email: [privacy@avehealthpartners.com] Phone: [Phone Number]

This Privacy Policy is a general template intended to reflect common HIPAA and North Carolina legal requirements applicable to health-data analytics services. It does not constitute legal advice. Ave Health Partners, Inc. should have this Policy reviewed and finalized by qualified legal counsel to confirm its accuracy and completeness in light of the company's specific data flows, client agreements, HIPAA status (covered entity vs. business associate), and any other applicable state or federal laws.