AVE HEALTH PARTNERS, INC.

DATA COLLECTION, USE, AND PRIVACY POLICY

Governing the Collection, Storage, Use, and Protection of Personal and Health Information

Effective Date: [●], 2026

Last Reviewed: [●], 2026

Policy Owner: Privacy Officer / HIPAA Security Officer

CONFIDENTIAL — INTERNAL AND CLIENT-FACING GOVERNANCE DOCUMENT

This is a template policy prepared for general informational purposes. It is not legal advice. Ave Health Partners, Inc. should have this document reviewed and adapted by North Carolina–licensed legal counsel and its HIPAA Privacy/Security Officer before adoption, and should update it as its services, technology, and applicable law evolve.

TABLE OF CONTENTS

1. Purpose and Scope

This Data Collection, Use, and Privacy Policy ("Policy") describes how Ave Health Partners, Inc. ("Ave Health Partners," the "Company," "we," "us," or "our") collects, uses, stores, analyzes, discloses, and protects personal information and personal health information in connection with its wearable-device integration, patient/client health data intake, electronic medical record ("EMR") interfaces, third-party laboratory connections, health analytics, and custom reporting services (collectively, the "Services").

This Policy applies to all personal information and health data the Company collects from or about individuals who use the Services ("Clients," "Patients," or "Users"), regardless of whether the data is collected directly, through a connected wearable or Bluetooth-enabled device, through a client-authorized EMR interface, through a third-party laboratory, or entered manually by the individual.

This Policy applies to all Company workforce members, contractors, subcontractors, and Business Associates (as defined below) who create, receive, maintain, transmit, or have access to such data on the Company's behalf.

Data Ownership. As between the Company and the Client, the Client retains ownership of the Client's personal information and personal health data. The Company acts as custodian and processor of that data for the purposes described in this Policy and in the applicable client services agreement or Business Associate Agreement ("BAA"), and does not claim ownership of underlying Client data. This ownership structure does not limit the Company's own rights in de-identified, aggregated data or in the analytical methods, algorithms, and report templates it develops, as further described in Section 8.

2. Definitions

- "Personal Information" means information that identifies, relates to, or could reasonably be linked with a particular individual, such as name, address, date of birth, contact details, or government-issued identification numbers.
- "Protected Health Information" or "PHI" has the meaning given in the HIPAA Privacy Rule, 45 C.F.R. § 160.103 — individually identifiable health information transmitted or maintained in any form or medium.
- "Electronic PHI" or "ePHI" means PHI that is transmitted by or maintained in electronic media, as defined at 45 C.F.R. § 160.103.
- "Wearable/Bluetooth Device Data" means biometric and physiological data transmitted from a consumer wearable, fitness tracker, or Bluetooth-enabled medical or health monitoring device connected to the Services.
- "Business Associate" has the meaning given in 45 C.F.R. § 160.103 and includes any third-party laboratory, cloud hosting provider, analytics subcontractor, or other vendor that creates, receives, maintains, or transmits PHI on the Company's behalf.
- "De-Identified Data" means health information that no longer identifies an individual and for which there is no reasonable basis to believe it can be used to identify an individual, de-identified in accordance with 45 C.F.R. § 164.514.
- "Custom Report" means an analytical output — such as a trend analysis, risk score, or summary dashboard — that the Company generates for a Client by processing the data categories described in Section 3.

3. Categories of Data We Collect

The Company collects the following categories of personal information and health data in order to provide the Services:

Data Category	Examples of Data Collected
Identifying / Contact Information	Name, date of birth, address, phone number, email address, government-issued identification numbers, insurance identification numbers, and emergency contact information.
Wearable & Bluetooth-Enabled Device Data	Heart rate, heart rate variability, blood oxygen saturation, sleep patterns, step counts, activity levels, blood glucose readings, blood pressure, body temperature, ECG/EKG readings, and device identifiers transmitted from consumer wearables and Bluetooth-enabled medical devices.
Client / Patient-Supplied Data	Self-reported symptoms, medical history, medication lists, allergies, nutrition and lifestyle information, survey and questionnaire responses, and information entered directly into Company applications or portals.
Electronic Medical Record (EMR) Data	Diagnoses, clinical notes, treatment history, immunization records, and other protected health information obtained from client-authorized EMR/EHR systems.
Third-Party Laboratory Data	Laboratory test orders and results, biomarker panels, genetic or genomic testing results (where applicable), and related diagnostic data received from contracted clinical laboratories.
Derived / Analytical Data	Custom health reports, trend analyses, risk scores, and other insights the Company generates by analyzing the categories of data above.
Technical & Usage Data	IP address, device and browser type, application log data, and authentication records associated with access to the Company's platform.

3.1 How Data Is Collected

- Directly from Clients and Patients through onboarding forms, intake questionnaires, and the Company's web or mobile applications.
- Automatically from wearables and Bluetooth-enabled devices that a Client or Patient authorizes to sync with the Services.
- From EMR/EHR systems, pursuant to the Client's authorization and, where applicable, a data-sharing or interoperability agreement with the EMR vendor or health system.
- From contracted third-party clinical laboratories that transmit test orders and results pursuant to a Business Associate Agreement.
- Automatically through the Company's platform in the form of technical and usage data (e.g., log files, device identifiers, authentication records).

4. Legal and Regulatory Framework

The Company collects, uses, and safeguards data described in this Policy in accordance with applicable federal and North Carolina law, including but not limited to:

4.1 Federal Law

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the HIPAA Privacy Rule (45 C.F.R. Part 160 and Subparts A and E of Part 164), the HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164), and the HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D).

- The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which extends HIPAA obligations to Business Associates and strengthens breach notification and enforcement requirements.
- Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), prohibiting unfair or deceptive acts or practices, and the FTC Health Breach Notification Rule (16 C.F.R. Part 318) applicable to certain non-HIPAA-covered consumer health record and wearable data.
- The 21st Century Cures Act information-blocking provisions and related interoperability rules, to the extent applicable to the Company's EMR interfaces.
- Applicable federal genetic information nondiscrimination and clinical laboratory requirements (e.g., GINA and CLIA), where the Services involve laboratory-derived or genetic data.

4.2 North Carolina Law

- The North Carolina Identity Theft Protection Act, N.C. Gen. Stat. Chapter 75, Article 2A (N.C. Gen. Stat. §§ 75-60 through 75-66), which governs the safeguarding, use, and disposal of personal identifying information and requires notification to affected North Carolina residents and the North Carolina Attorney General's Consumer Protection Division following a qualifying security breach, and generally requires that notification occur without unreasonable delay (N.C. Gen. Stat. § 75-65).
- N.C. Gen. Stat. § 75-1.1 (Unfair and Deceptive Trade Practices Act), which the North Carolina Attorney General and private plaintiffs may invoke for violations of the Identity Theft Protection Act's notification requirements.
- North Carolina statutes and common-law principles governing the confidentiality of medical records and communications, including protections applicable to hospital, physician, and other licensed provider records with which the Company's EMR interfaces may interact.
- North Carolina data-disposal and Social Security number handling restrictions under the Identity Theft Protection Act, which govern how the Company and its vendors must destroy or redact records containing such identifiers when no longer needed.

Because North Carolina does not currently have a comprehensive consumer data privacy statute of general application (unlike, for example, California or Virginia), the Company's baseline privacy and security obligations for health data are principally governed by HIPAA/HITECH at the federal level and by the Identity Theft Protection Act at the state level. The Company monitors pending North Carolina legislation and will update this Policy if a comprehensive state privacy law is enacted.

5. Consent and Client Authorization

Before collecting data under this Policy, the Company obtains appropriate authorization, which may include one or more of the following depending on the data source and applicable law:

1. A signed HIPAA-compliant authorization (45 C.F.R. § 164.508) or, where the Company or a Client is acting as a covered entity's Business Associate, coverage under an executed Business Associate Agreement and the covered entity's Notice of Privacy Practices.
2. Affirmative consent within the Company's application or portal at the time a Client or Patient connects a wearable or Bluetooth-enabled device, describing the categories of data to be synced.
3. Written or electronic authorization permitting the Company to request records from a named EMR system, health system, or provider.
4. Authorization permitting a contracted laboratory to transmit test orders and results to the Company on the Client's behalf.

Clients and Patients may withdraw consent for future data collection at any time by contacting the Company as described in Section 14, subject to the Company's and any covered entity's obligation to retain records already created in accordance with applicable law and Section 10 of this Policy.

6. How We Use Health Data — Analytics and Custom Reports

The Company analyzes the data described in Section 3 to generate Custom Reports and related analytical outputs for the Client that ordered them, including trend analysis, risk indicators, and consolidated views that combine wearable, EMR, patient-supplied, and laboratory data. The Company uses this data only for the following purposes:

- Providing, maintaining, and improving the Services requested by the Client, including generating Custom Reports.
- Verifying the identity of Clients and Patients and administering their accounts.
- Coordinating with the Client's authorized providers, laboratories, and EMR systems to obtain and reconcile data.
- Complying with legal, regulatory, and contractual obligations, including responding to lawful requests from regulators or law enforcement.
- Internal quality assurance, security monitoring, and audit logging.
- Creating de-identified, aggregated data sets for internal analytics, product improvement, or research, in accordance with the de-identification standards of 45 C.F.R. § 164.514.

The Company does not sell Client or Patient personal health data. The Company does not use PHI for marketing purposes without separate, specific authorization, consistent with the HIPAA Privacy Rule's requirements for marketing communications (45 C.F.R. § 164.508(a)(3)).

7. Data Storage, Cloud Hosting, and Security Safeguards

Secure Cloud Storage. All Client and Patient data described in this Policy is stored in a HIPAA-compliant cloud database environment operated by a cloud services provider that has executed a Business Associate Agreement with the Company. Data is stored in facilities located within the United States unless otherwise disclosed to and authorized by the Client.

7.1 Administrative Safeguards

- A designated HIPAA Privacy Officer and Security Officer responsible for developing, implementing, and enforcing this Policy and related procedures.
- Workforce training on HIPAA, this Policy, and data handling procedures at onboarding and at least annually thereafter.
- Role-based access controls limiting access to PHI and personal information to workforce members and systems with a legitimate business need ("minimum necessary" standard, 45 C.F.R. § 164.502(b)).
- Written Business Associate Agreements with all vendors, including the cloud hosting provider, analytics subcontractors, and third-party laboratories, that create, receive, maintain, or transmit PHI on the Company's behalf.
- A documented incident response and breach notification procedure, described in Section 9.

7.2 Physical Safeguards

- Data centers used by the Company's cloud provider maintain physical access controls, environmental protections, and facility security consistent with HIPAA Security Rule requirements (45 C.F.R. § 164.310).

- Company workstations and devices used to access PHI are subject to physical security controls, including workstation locking and restricted physical access.

7.3 Technical Safeguards

- Encryption of ePHI both in transit (e.g., TLS 1.2 or higher) and at rest (e.g., AES-256 or equivalent), consistent with 45 C.F.R. § 164.312(a)(2)(iv) and (e)(2)(ii).
- Unique user authentication and, where applicable, multi-factor authentication for all systems that access PHI.
- Automatic session logoff and audit logging of access to, and modification of, ePHI, consistent with 45 C.F.R. § 164.312(b).
- Network security controls, including firewalls, intrusion detection/prevention, and periodic vulnerability scanning and penetration testing.
- Secure, encrypted data transmission protocols for wearable/Bluetooth device syncing, EMR interfaces, and laboratory data feeds.
- Regular data backups and a documented disaster recovery and contingency plan (45 C.F.R. § 164.308(a)(7)).

The Company conducts periodic HIPAA risk assessments of its systems, including its cloud hosting environment, and remediates identified vulnerabilities in accordance with a risk-based priority schedule.

8. Data Sharing, Business Associates, and Third-Party Laboratories

The Company does not disclose Client or Patient personal information or PHI to third parties except as described below or as otherwise authorized in writing by the Client or Patient:

- Business Associates. The Company shares data with vendors — including its cloud hosting provider, analytics infrastructure providers, and other service providers — that perform functions on the Company's behalf, each of which is bound by a Business Associate Agreement imposing HIPAA-equivalent safeguards and use restrictions.
- Third-Party Laboratories. The Company exchanges data with contracted clinical laboratories to obtain test orders and results under a Business Associate Agreement or equivalent data-sharing agreement, limited to the data necessary to fulfill the ordered testing and reporting.
- EMR/EHR Systems. The Company exchanges data with EMR systems and health information networks only as authorized by the Client and subject to applicable interoperability and data-sharing agreements.
- Legal and Regulatory Disclosures. The Company may disclose data where required by law, court order, or regulatory demand, or as otherwise permitted under the HIPAA Privacy Rule (e.g., 45 C.F.R. § 164.512), including breach reporting obligations to the North Carolina Attorney General's office described in Section 9.
- De-Identified and Aggregated Data. The Company may share de-identified, aggregated data that does not identify any individual for research, product improvement, or benchmarking purposes.

The Company does not sell personal information or PHI, and does not permit Business Associates or third-party laboratories to use Client or Patient data for their own independent marketing purposes.

Analytical Outputs and Intellectual Property. While underlying Client data remains the property of the Client as described in Section 1, the Company retains ownership of its proprietary analytics methodologies, algorithms, scoring models, and report templates used to generate Custom Reports, independent of the underlying data to which they are applied.

9. Security Incident and Breach Notification Procedures

The Company maintains a documented security incident response plan designed to detect, contain, investigate, and remediate suspected or actual unauthorized access to, or acquisition, use, or disclosure of, personal information or PHI. In the event of a breach affecting unsecured PHI or personal information, the Company will:

5. Investigate and document the scope of the incident, including the categories of data and individuals affected.
6. Notify affected individuals without unreasonable delay, and in any event consistent with the timing requirements of the HIPAA Breach Notification Rule (45 C.F.R. §§ 164.404–164.408, generally no later than 60 calendar days after discovery for HIPAA-covered breaches) and the North Carolina Identity Theft Protection Act's "without unreasonable delay" standard (N.C. Gen. Stat. § 75-65).
7. Notify the U.S. Department of Health and Human Services Office for Civil Rights as required under the HIPAA Breach Notification Rule.
8. Notify the North Carolina Attorney General's Consumer Protection Division without unreasonable delay when a breach affects North Carolina residents, and notify nationwide consumer reporting agencies where the breach affects more than 1,000 individuals at one time, consistent with N.C. Gen. Stat. § 75-65.
9. Notify affected Clients so that Clients may satisfy any notification obligations they independently owe as a covered entity or data owner.
10. Cooperate with law enforcement and permit a reasonable delay in notification where a law enforcement agency determines that notification would impede a criminal investigation.

Business Associates and subcontractors, including the Company's cloud hosting provider and contracted laboratories, are contractually required to report any suspected or actual breach of unsecured PHI to the Company without unreasonable delay so that the Company can meet the timelines above.

10. Data Retention and Disposal

The Company retains personal information and PHI only for as long as necessary to provide the Services, satisfy the purposes described in this Policy, and comply with applicable legal, regulatory, and contractual retention requirements, including HIPAA's six-year documentation retention requirement (45 C.F.R. § 164.316(b)(2)) and any longer retention period required by North Carolina medical records or laboratory recordkeeping requirements.

Upon expiration of the applicable retention period, or upon a Client's validly authorized request and subject to any legal hold or independent retention obligation, the Company will securely destroy or de-identify the data using methods consistent with NIST guidance and North Carolina's Identity Theft Protection Act disposal requirements, such as cryptographic erasure, secure wipe, or physical destruction of storage media.

11. Individual Rights

Subject to the Client's role as data owner and any applicable covered-entity relationship, individuals whose data the Company processes generally have the right to:

- Request access to, and a copy of, their personal information and PHI held by the Company, consistent with the HIPAA right of access (45 C.F.R. § 164.524).
- Request an amendment or correction of inaccurate or incomplete information (45 C.F.R. § 164.526).
- Request an accounting of certain disclosures of PHI (45 C.F.R. § 164.528).
- Request restrictions on certain uses or disclosures of PHI, and request confidential communications (45 C.F.R. §§ 164.522(a)-(b)).
- Withdraw a previously granted authorization for future data collection, as described in Section 5.

- File a complaint with the Company's Privacy Officer, the U.S. Department of Health and Human Services Office for Civil Rights, or the North Carolina Attorney General's Consumer Protection Division.

Requests should be directed to the Company's Privacy Officer using the contact information in Section 14. The Company will respond within the timeframes required by HIPAA and applicable law.

12. Workforce Access, Training, and Accountability

- Access to personal information and PHI is limited to workforce members whose job functions require it, based on the minimum necessary standard.
- All workforce members and contractors with access to PHI complete HIPAA privacy and security training at onboarding and at least annually, and sign confidentiality agreements.
- Workforce members must report suspected privacy or security incidents immediately to the Privacy Officer or Security Officer.
- Violations of this Policy may result in disciplinary action, up to and including termination, and, where applicable, referral to law enforcement or regulatory authorities.

13. Policy Review and Amendments

The Company will review this Policy at least annually and whenever there is a material change in the Services, applicable law, or the Company's data processing practices, including changes to HIPAA, HITECH, FTC rules, or North Carolina law (including any future comprehensive North Carolina consumer privacy statute). Material changes will be communicated to Clients in accordance with the applicable services agreement and, where required, through an updated Notice of Privacy Practices.

14. Contact Information

Privacy Officer / HIPAA Security Officer: [Name / Title]

Ave Health Partners, Inc.

Address: [Street Address, Suite, City, North Carolina, ZIP]

Phone: [Phone Number]

Email: [privacy@avehealthpartners.com]

Individuals may also file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, or with the North Carolina Attorney General's Consumer Protection Division, without retaliation from the Company.

This document is a template for internal drafting purposes only and does not constitute legal advice. Ave Health Partners, Inc. should engage North Carolina–licensed legal counsel to review and finalize this Policy, its Notice of Privacy Practices, and its Business Associate Agreements before adoption or distribution to Clients.