AVE HEALTH PARTNERS, INC.

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL AND HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Effective Date: [●], 2026

Last Reviewed / Revised: [●], 2026

Version applies to all Ave Health Partners, Inc. wearable, patient-supplied, EMR-connected, laboratory, and health analytics services.

This Notice is a template prepared for general informational purposes and is not legal advice. Ave Health Partners, Inc. should have this Notice reviewed by North Carolina–licensed legal counsel and its HIPAA Privacy Officer before distribution to Clients and Patients, and should update it as its services, technology, and applicable law evolve.

1. Our Commitment to Your Privacy

Ave Health Partners, Inc. ("Ave Health Partners," the "Company," "we," "us," or "our") provides health data collection, integration, and analytics services, including the collection of data from wearable and Bluetooth-enabled devices, patient-supplied information, Electronic Medical Records ("EMR"), and third-party clinical laboratories, and the creation of custom analytical health reports for our Clients. In the course of providing these services, we create, receive, maintain, and transmit protected health information ("PHI") as that term is defined under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA").

We are required by law to maintain the privacy and security of your PHI, to provide you with this Notice describing our legal duties and privacy practices with respect to your PHI, to notify affected individuals following a breach of unsecured PHI, and to abide by the terms of this Notice currently in effect.

As between Ave Health Partners and the Client on whose behalf we provide services, the Client retains ownership of the underlying personal information and health data described in this Notice. Ave Health Partners acts as custodian and, where applicable, as a Business Associate or covered entity with respect to that data, consistent with our services agreement and any Business Associate Agreement ("BAA") in place.

2. The Health Information Covered by This Notice

This Notice applies to PHI we create or receive on your behalf, including:

- Identifying and contact information, such as your name, date of birth, address, and insurance information.
- Biometric and physiological data transmitted from wearable devices and Bluetooth-enabled medical or fitness devices you connect to our Services (for example, heart rate, blood oxygen, sleep, activity, blood glucose, or blood pressure readings).
- Information you supply directly, such as symptoms, medical history, medications, allergies, and questionnaire responses.
- Records obtained from Electronic Medical Record / Electronic Health Record systems that you or your provider have authorized us to access.
- Laboratory orders and results received from contracted third-party clinical laboratories.
- Custom health reports, trend analyses, and other outputs we generate by analyzing the categories of information above.

3. How We May Use and Disclose Your Health Information Without Your Written Authorization

The following categories describe the ways we are permitted to use and disclose your PHI without your written authorization. Not every use or disclosure in each category is described, but the permitted uses and disclosures fall into one of these categories.

3.1 For Treatment

We may use and disclose your PHI to coordinate and manage the health-related services provided to you, including sharing information among your authorized providers, our analytics staff, and the laboratories or EMR systems connected to your account.

> ***Example:*** *We combine data synced from your wearable device with results received from your laboratory and your EMR to generate a custom report that we deliver to you or your treating provider.*

3.2 For Payment

We may use and disclose your PHI as necessary to obtain payment for the Services, such as submitting information to your health plan, verifying coverage, or billing for laboratory or analytics services rendered on your behalf.

3.3 For Health Care Operations

We may use and disclose your PHI to support our own operations and to support the operations of Clients for whom we provide services, including quality assessment, staff training, compliance and audit activities, and business planning.

> ***Example:*** *We may review de-identified trends across our Client base to improve the accuracy of our analytics models and report templates.*

3.4 Other Permitted or Required Uses and Disclosures Without Authorization

We may also use or disclose your PHI, without your written authorization, in the following circumstances, each of which is subject to specific conditions under HIPAA (45 C.F.R. § 164.512):

- As Required by Law — when disclosure is required by federal, state, or local law, including North Carolina law.
- Public Health Activities — such as reporting to public health authorities for disease prevention or control, or reporting device-related adverse events to the FDA.
- Health Oversight Activities — to health oversight agencies for audits, investigations, licensure, or other oversight activities authorized by law.
- Judicial and Administrative Proceedings — in response to a court order, subpoena, or other lawful process, subject to applicable legal requirements.
- Law Enforcement Purposes — in limited circumstances, such as in response to a valid legal process or to report certain types of wounds or injuries as required by North Carolina law.
- To Avert a Serious Threat to Health or Safety — to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
- Research — for research purposes, subject to a waiver or alteration of authorization approved by an Institutional Review Board or Privacy Board, or in a manner that does not identify you.
- Workers' Compensation — as authorized by, and to the extent necessary to comply with, North Carolina workers' compensation laws.
- Business Associates — with vendors that perform functions on our behalf, including our HIPAA-compliant cloud hosting provider, analytics infrastructure providers, and contracted laboratories, each of which is bound by a Business Associate Agreement requiring it to safeguard your information.
- Decedents, Organ Donation, Coroners, and Medical Examiners — as permitted by law.
- Military, National Security, and Correctional Institutions — in limited circumstances specified by law.

We will never sell your PHI, and we will not use your PHI for marketing purposes, without your specific written authorization, consistent with 45 C.F.R. § 164.508.

4. Uses and Disclosures That Require Your Written Authorization

Other than as described in Section 3, we will use or disclose your PHI only with your written authorization, including for purposes such as:

- Marketing communications about products or services, where such communications constitute marketing under HIPAA.
- Sale of your PHI to a third party.

- Disclosure of psychotherapy notes, if applicable to your records.
- Any other use or disclosure not otherwise described in this Notice.

You may revoke a written authorization at any time by submitting a written request to our Privacy Officer, except to the extent we have already relied on the authorization or if the authorization was obtained as a condition of obtaining insurance coverage and other law permits the insurer to contest a claim under the policy.

5. Your Rights Regarding Your Health Information

You have the following rights with respect to the PHI we maintain about you. To exercise any of these rights, please submit a written request to our Privacy Officer using the contact information in Section 10.

5.1 Right to Access and Obtain a Copy

You have the right to inspect and obtain a copy of your PHI, including data synced from wearable and Bluetooth-enabled devices, patient-supplied data, EMR data, laboratory results, and Custom Reports, in the form and format you request if readily producible, consistent with 45 C.F.R. § 164.524. We will respond to your request within the time required by law, generally no later than 30 calendar days, with one 30-day extension permitted upon written notice. We may charge a reasonable, cost-based fee for copies.

5.2 Right to Request Amendment

You have the right to request that we amend your PHI if you believe it is inaccurate or incomplete, consistent with 45 C.F.R. § 164.526. We may deny your request under certain circumstances, such as if we did not create the information or believe it is accurate and complete; if we deny your request, we will explain the reason in writing and you may submit a statement of disagreement.

5.3 Right to an Accounting of Disclosures

You have the right to receive a list of certain disclosures we have made of your PHI, generally covering the six years prior to your request, subject to the exceptions in 45 C.F.R. § 164.528 (for example, disclosures made for treatment, payment, or health care operations, or made pursuant to your authorization, are generally excluded).

5.4 Right to Request Restrictions

You have the right to request restrictions on how we use or disclose your PHI for treatment, payment, or health care operations, and on disclosures to persons involved in your care. We are not required to agree to a requested restriction, except that we must agree to restrict disclosure to a health plan for payment or health care operations purposes if the disclosure relates solely to a service you paid for out of pocket in full, consistent with 45 C.F.R. § 164.522(a).

5.5 Right to Request Confidential Communications

You have the right to request that we communicate with you about your PHI by alternative means or at an alternative location (for example, only by email or only to a specific address), and we will accommodate reasonable requests.

5.6 Right to Notice of a Breach

You have the right to be notified if we discover a breach of your unsecured PHI, consistent with the HIPAA Breach Notification Rule (45 C.F.R. §§ 164.404–164.408) and, for North Carolina residents, the notification standards of the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-65.

5.7 Right to a Paper Copy of This Notice

You have the right to receive a paper copy of this Notice at any time, even if you agreed to receive it electronically.

5.8 Right to Choose Someone to Act on Your Behalf

If you have given someone medical power of attorney or if someone is your legal guardian, that person may exercise your rights and make choices about your PHI. We will verify that the person has this authority before taking action.

6. Our Responsibilities

- We are required by law to maintain the privacy and security of your PHI.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your PHI.
- We must follow the duties and privacy practices described in this Notice and give you a copy of it.
- We will not use or share your PHI other than as described here unless you tell us we can in writing; you may revoke that written permission at any time, as described in Section 4.
- We store your PHI in a HIPAA-compliant, encrypted cloud database, and require our cloud hosting provider, laboratory partners, and other vendors that handle your PHI to sign Business Associate Agreements obligating them to protect your information to the same standard.

7. Changes to This Notice

We reserve the right to change the terms of this Notice, and the changes will apply to all PHI we already have about you as well as any information we receive in the future. We will make the revised Notice available upon request, post it in a location where Clients and Patients can readily access it (such as our Client portal), and, where required by law, provide it to you directly. The current Effective Date is noted on the cover of this Notice.

8. North Carolina Law and Additional Protections

In addition to the federal HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, Ave Health Partners' privacy and security practices are informed by North Carolina law, including:

- 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 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 without unreasonable delay following a qualifying security breach (N.C. Gen. Stat. § 75-65).
- North Carolina statutes and common-law protections applicable to the confidentiality of medical records maintained by licensed health care providers and facilities with which our EMR interfaces may connect.
- Where North Carolina law provides greater privacy protection than HIPAA for a particular category of information (for example, certain communicable disease, HIV/AIDS, genetic testing, or mental health and substance use records), we will apply the more protective standard to the extent it applies to the information we hold.

North Carolina does not currently have a comprehensive consumer data privacy statute of general application. If one is enacted, we will update this Notice as necessary to reflect any additional rights it provides to North Carolina residents.

9. Complaints

If you believe your privacy rights have been violated, you may file a complaint with our Privacy Officer using the contact information below, or with the U.S. Department of Health and Human Services, Office for Civil Rights, or the

North Carolina Attorney General's Consumer Protection Division. You will not be retaliated against for filing a complaint.

U.S. Department of Health and Human Services, Office for Civil Rights: 200 Independence Avenue, S.W., Washington, D.C. 20201; (800) 368-1019; www.hhs.gov/ocr/privacy/hipaa/complaints

North Carolina Attorney General, Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699-9001; (877) 566-7226

10. Contact Us

If you have questions about this Notice, or to exercise any of the rights described above, please contact:

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]

This Notice 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 Notice, and should confirm consistency with its internal Data Collection Policy, Business Associate Agreements, and services agreements before adoption or distribution to Clients and Patients.