Included Health Privacy Policy

Effective Date: February 1, 2026

This policy describes how Included Health, Inc. and its associated entities ("Included Health," "we," "us," or "our") collect, use, disclose, and protect personal information across our websites, mobile applications, and products and services that link to this Privacy Policy (collectively, the "Sites").
Our purpose is to:

- Ensure clear understanding of how Included Health processes personal and health-related information
- Demonstrate compliance with HIPAA, CCPA/CPRA, and other applicable U.S. privacy laws; and
- Reaffirm Included Health's commitment to transparency, trust, and responsible data stewardship.

Included Health, Inc. ("Included Health", "Company", "we", "us", or "our") operates the websites located at includedhealth.com and doctorondemand.com, and other websites, products, services, and mobile applications with links to this Privacy Policy, including without limitation, the Doctor On Demand webpages and secure applications (collectively, the "Sites" or "Websites", unless otherwise specified). Users of the Sites or Services are referred to below as "Users", "Members", "you", "your", or "yours".

We offer online telehealth services enabling our Members to report their health history and engage independent healthcare professionals ("Healthcare Professionals") to obtain medical and healthcare services, as well as provide behavioral health coaching from Coaches ("Coaches") who do not provide professional or clinical services.

The Healthcare Professionals who deliver Services through Included Health are independent professionals practicing within several groups of independently owned professional practices (collectively, "Doctor On Demand Professionals"). Please refer to the Doctor On Demand Professionals Notice of Privacy Practices to learn more about these groups and how they're organized.

Please note that Users in different regions may be subject to different data protection laws, regulations, and standards. As such, this document has a section dedicated to California consumers, as well as a section dedicated to consumers subject to European Union jurisdiction.

Please read this Privacy Policy carefully before using the Sites or Services. By visiting or using any of the Sites or Services, you are accepting the practices described in this Privacy Policy, as well as the Included Health Terms of Service and other terms, agreements, statements of rights, consent forms, and policies referenced above, as applicable.

Geographic Scope: Included Health's services are intended for individuals located in the United States, and we primarily process personal information in accordance with applicable U.S. privacy and healthcare laws. If we become subject to non-U.S. data protection laws in connection with specific users, services, or processing activities, we will comply with those laws as required.
State Coverage: This policy is designed for operations in all 50 U.S. states and incorporates heightened protections required under applicable state privacy laws .

1. Information We Collect

We collect the following categories of information from Members, users, employers, and plan partners:

- Identifiers: Name, address, email, phone number, date of birth, SSN (last four digits only, where required for identity verification or plan administration and permitted by law).
- Demographic and Eligibility Information: Employer or plan details, coverage information, benefit eligibility, and member ID numbers.
- Health Information: Medical history, symptoms, diagnoses, prescriptions, clinical notes, claims data, and provider correspondence.
- Technical and Usage Data: IP address, device type, browser type, mobile ID, cookies, beacons, and other analytics information.
- Correspondence and Interaction Data: Messages, support requests, or chat interactions via our apps or member portal.

We collect information directly from you, from your health plan or employer (where permitted by law or contract), from your clinicians, and through technologies that support our platform.

2. Use of Information

We use PII and PHI for lawful business purposes including:

- Delivering and coordinating clinical and telehealth services;
- Managing member accounts and customer support;
- Processing payments and insurance claims;
- Conducting analytics for healthcare operations, quality improvement, population health management, and service optimization, as permitted under HIPAA and applicable law;
- Communicating about benefits, programs, and service updates;
- Protecting against fraud, security threats, or illegal activities; and
- Meeting legal or regulatory requirements.

We do not use or disclose PHI for marketing or sales purposes without your authorization.

3. Disclosure of Information

We may share information as follows:

Category	Purpose
With Health Care Providers and Plans	For treatment, payment, and health-care operations under HIPAA.
With Vendors and Business Associates	To perform services on our behalf (e.g., hosting, IT security, claims support). All vendors must sign Business Associate Agreements and adhere to HIPAA.
With Employers or Benefit Sponsors	Limited to aggregated, de-identified data unless otherwise authorized or required by law; except where individual-level information is required to administer benefits, coordinate care, or as authorized by the Member or required by law.
With Law Enforcement or Regulators	As required by law, court order, or subpoena.
For Corporate Transactions	As part of a merger, acquisition, or asset transfer subject to confidentiality protections.
For Legal and Compliance Purposes	To enforce rights, prevent fraud, and comply with applicable laws.

We do not sell Member data and do not share PHI with data brokers or advertising platforms.

4. HIPAA Compliance

When Included Health acts as a covered entity or business associate, we handle PHI in accordance with HIPAA Privacy, Security, and Breach Notification Rules and our Business Associate Agreements.

We maintain HIPAA-compliant security controls, including encryption in transit and (where appropriate) at rest, access logging, auditing, and employee training.

5. California and State Consumer Privacy Rights

Residents of certain states have additional rights. For California residents under the CCPA/CPRA, and other states with comparable laws:

You may have the right to:

- Know what personal information we collect and how we use it;
- Request access to or deletion of personal information;
- Correct inaccurate personal information;
- Opt out of the “sale” or “sharing” of personal information (as defined under applicable state law); and

- Limit use of sensitive personal information where required by law.

Included Health does not sell personal information. Certain third-party cookie or analytics tools may constitute a “sale” or “share” under state law; users may opt out via the “Do Not Sell or Share My Data” link on our Sites. We also honor opt-out preference signals where required by law.

Requests to exercise these rights must be verifiable and submitted through our privacy portal or by contacting privacy@includedhealth.com. We respond within statutory deadlines (typically 45 days, extendable to 90 days with notice).

Sensitive Personal Information:
For purposes of applicable state privacy laws (including the California Privacy Rights Act), Sensitive Personal Information (“SPI”) includes personal information that reveals or relates to:

- A consumer’s Social Security number, driver’s license number, state identification card number, or passport number;
- A consumer’s account log-in, financial account, debit card, or credit card number, in combination with any required security or access code, password, or credentials allowing access to an account;
- A consumer’s precise geolocation;
- A consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer’s mail, email, or text messages, unless Included Health is the intended recipient of the communication;
- A consumer’s genetic data or biometric information used for uniquely identifying a consumer; and
- A consumer’s health information, including medical conditions, diagnoses, treatment information, and other information subject to HIPAA or similar healthcare privacy laws.

Where required by law, you may have the right to limit the use and disclosure of Sensitive Personal Information to purposes permitted by applicable law, such as providing healthcare services, maintaining account security, complying with legal obligations, and other necessary business and operational purposes.

Appeals. Where required by applicable state law, you may appeal our decision regarding your privacy rights request. Instructions for submitting an appeal will be provided with our response. We will respond to appeals within the timeframe required by law.

6. Data Security

We maintain reasonable administrative, technical, and physical safeguards to protect PII and PHI from unauthorized access or disclosure, including:

- Multi-factor authentication and least-privilege access controls;
- Continuous monitoring and encryption of data in transit and at rest;
  Vendor risk management and security due diligence;
  Incident response and breach notification protocols; and
- Annual training and testing for workforce members.

No system is completely secure; however, we follow current HHS and NIST best practices and conduct regular risk assessments.

7. Data Retention and Destruction

Personal information is retained only for as long as necessary to fulfill its purpose, comply with legal obligations, resolve disputes, and enforce agreements. PHI is retained in accordance with federal and state record-retention requirements. HIPAA administrative documentation is retained for at least six years, and medical and clinical records are retained in accordance with applicable federal and state medical record retention requirements, which may be longer. . Data is securely destroyed or de-identified when no longer needed.

8. Breach Notification

If a breach of unsecured PHI or PII occurs, we will notify affected individuals and regulators without unreasonable delay and within the timeframes required by applicable federal and state law. Vendors and business associates must report any incident to Included Health within 24 hours of discovery in accordance with the 2025 HHS Security Rule update.

9. Workforce Responsibilities

Included Health maintains workforce training and internal reporting mechanisms to support compliance with privacy and security requirements.

10. Policy Governance and Administration

The Chief Compliance Officer (CCO) oversees this policy and approves updates in consultation with Legal and Information Security. The CCO conducts biennial reviews (or more frequently if laws change) and monitors implementation through periodic audits and risk assessments.

11. Exercising Privacy Rights

Requests to access, amend, delete, or restrict information must be submitted through:

- Member portal (chat or open case feature), or
- Email to privacy@includedhealth.com with identity verification steps.

We respond to HIPAA access requests within 30 days, with one permitted extension as allowed by law, and to consumer privacy requests within 45 days (extendable to 90 with notice).