b.well

Published: June 5, 2026
Last Revised: See Revision History
Incorporated into: health.network Startup Terms of Service — Startup Package

health.network
Data Processing Addendum (DPA)

This Data Processing Addendum ("DPA" or "Addendum") is incorporated by reference into the health.network Startup Terms of Service (the "Agreement") between b.well Connected Health, Inc. ("b.well") and Customer. Together with the Agreement, the Order Form, and the b.well Acceptable Use Policy (AUP), this DPA constitutes the complete data processing framework governing b.well's Processing of Personal Data on Customer's behalf.

This DPA applies wherever b.well Processes Personal Data as a processor or service provider acting on Customer's instructions. It does not govern b.well's use of De-Identified Data, AI Development Purposes data processed under ToS Section 6, or data for which b.well acts as an independent controller under Applicable Data Protection Law.

Capitalized terms not defined in this DPA have the meanings assigned in the Agreement (including Exhibit A — Definitions). In the event of any conflict, this DPA controls over the Agreement with respect to the Processing of Personal Data.

1. Roles and Processing Instructions

Customer is and shall remain the controller of all Personal Data provided to or accessed by b.well under the Agreement. b.well shall act as a processor (or "service provider" under applicable U.S. state privacy law) and shall Process Personal Data only: (a) as necessary to perform its obligations and deliver the Products and Services under the Agreement; (b) in accordance with Customer's documented instructions; and (c) as required by Applicable Data Protection Law and governing frameworks for the exchange of health information.

Customer's execution of the Agreement and Order Form constitutes its documented instructions to b.well for Processing. Customer may provide additional written instructions from time to time; b.well will promptly notify Customer if it determines that any instruction violates Applicable Data Protection Law.

The subject matter, nature, purposes, duration, categories of data, and categories of Data Subjects applicable to Processing under this DPA are set forth in Schedule A (Processing Details) at the end of this document.

b.well's data use rights under ToS Section 6 (Data: Aggregation, Analysis, and AI) are separate from, and not limited by, this DPA. Those rights operate on the basis of b.well's independent authorization from Customer and Consumer End User consent, and are not Processing "on behalf of" Customer for purposes of this DPA.

2. Confidentiality of Personal Data

b.well will ensure that all personnel authorized to Process Personal Data are subject to appropriate confidentiality obligations, whether by contract or statutory requirement, and are trained on applicable data protection requirements. b.well will limit access to Personal Data to those personnel who require it to perform the Services.

3. Security

3.1 Information Security Program

b.well will implement and maintain a written Information Security Program comprising administrative, technical, and physical safeguards appropriate to the nature and sensitivity of the Personal Data Processed, including health data. These safeguards are designed to: (a) protect the confidentiality, integrity, and availability of Personal Data; (b) protect against reasonably anticipated threats and hazards; and (c) prevent unauthorized access, use, disclosure, alteration, or destruction of Personal Data. b.well may update its security safeguards from time to time, provided that updates do not materially reduce the overall level of protection.

3.2 Security Incident Notification

b.well will notify Customer without undue delay, and in any event within seventy-two (72) hours of discovery, of any confirmed unauthorized access, disclosure, loss, alteration, or destruction of Personal Data Processed on Customer's behalf (a "Security Incident"). Notification will include: (a) a description of the nature of the Security Incident; (b) the categories and approximate volume of Personal Data affected; (c) the likely consequences; and (d) the measures taken or proposed to address the incident. b.well will reasonably cooperate with Customer in investigating and remediating the Security Incident.

Notification of a Security Incident is not an acknowledgment of fault or liability by b.well.

4. Subprocessors

Customer grants b.well general authorization to engage Affiliates and third-party Subprocessors to assist in delivering the Services, subject to this Section. b.well's current list of Subprocessors is published and maintained at icanbwell.com/legal/sub-processors/ (last updated March 30, 2026).

b.well will: (a) enter into a written agreement with each Subprocessor imposing data protection obligations at least as protective as those in this DPA; (b) remain responsible to Customer for the Subprocessor's performance; and (c) provide Customer with at least ten (10) days' prior written notice before engaging a new Subprocessor or materially changing the role of an existing one, by updating the published Subprocessor list.

If Customer reasonably objects to a new or changed Subprocessor on data protection grounds, Customer will notify b.well in writing within ten (10) days of the published update. The Parties will work in good faith to resolve the objection. If no resolution is reached, Customer may terminate the Agreement upon thirty (30) days' written notice without liability for early termination.

5. Data Subject Rights

b.well will promptly notify Customer if b.well receives a request from a Data Subject seeking to exercise rights under Applicable Data Protection Law (e.g., access, correction, deletion, portability, or objection). b.well will not respond directly to such requests on Customer's behalf unless required by law or expressly instructed by Customer in writing.

b.well will provide Customer with reasonable technical and organizational assistance to enable Customer to fulfill Data Subject requests within applicable statutory timeframes, to the extent b.well can do so using the tools and information available to it. Customer is responsible for determining the applicable legal basis for each request and for communicating the outcome to the Data Subject.

For Consumer End User requests relating to data processed under ToS Section 6 (AI training, interaction data, de-identified data), b.well's obligations are governed by ToS Section 6.4 and b.well's published consumer-facing consent and rights mechanisms, not by this DPA.

6. Audit and Compliance Records

b.well will maintain records of its Processing activities as required by Applicable Data Protection Law. Upon thirty (30) days' prior written notice, Customer may request an audit of b.well's Processing activities once per calendar year to verify compliance with this DPA. Audits will be: (a) conducted at Customer's sole expense; (b) limited to information reasonably necessary to verify DPA compliance; (c) subject to the confidentiality provisions of the Agreement; and (d) conducted in a manner that minimizes disruption to b.well's operations.

Any independent auditor retained by Customer must execute a non-disclosure agreement with b.well on terms substantially similar to the Agreement's confidentiality provisions before commencing any audit.

b.well may satisfy its audit obligations by providing Customer with a current third-party audit report or security certification (e.g., SOC 2 Type II) in lieu of a Customer-conducted audit, where such report covers the scope of the requested audit.

7. Post-Termination Data Handling

Upon expiration or termination of the Agreement, b.well will, at Customer's election, either return or securely delete and destroy all Personal Data Processed on Customer's behalf within thirty (30) days, and provide written confirmation of such action upon request. b.well may retain: (a) backup or archival copies in accordance with its standard data retention schedule, which will be deleted as the schedule requires; and (b) Personal Data required to be retained by Applicable Law, which will be used only for the purpose that retention is required and subject to the confidentiality obligations of this DPA.

The data transfer obligations set forth in Order Form Section 5 (HL7 FHIR-compatible transfer for up to five business days) apply to Customer Data generally and are not modified by this DPA.

8. Limitation of Liability

The limitation of liability provisions set forth in Section 9 of the Agreement (Disclaimers and Limitations of Liability) apply in full to this DPA. No separate or higher liability cap applies to b.well's obligations under this DPA.

9. Updates to This DPA

b.well may update this DPA from time to time to reflect changes in Applicable Data Protection Law, b.well's products, or industry standards. Updates are effective upon posting at icanbwell.com/legal/health-network-startup-data-processing-addendum/. Customer's continued use of the Products and Services following the effective date of any update constitutes acceptance.

Schedule A — Processing Details

The following table describes the Processing of Personal Data performed by b.well on Customer's behalf under this DPA.

Controller: Customer	
Role	Controller of Personal Data provided to b.well under the Agreement
Obligations	Ensure a lawful basis for Processing; provide required notices to Data Subjects; instruct b.well on Processing; and comply with Applicable Data Protection Law
Processor: b.well Connected Health, Inc.	
Role	Processor acting on Customer's documented instructions
Processing purposes	Delivering the health.network Products and Services under the Agreement Operating the b.well Branded Experience, including Bailey™ integrations Platform analytics and improvement (as authorized under ToS Section 6) AI Development Purposes (as authorized under ToS Section 6.2–6.4, for Consented End User Data only) Subprocessor coordination and security operations Compliance with Applicable Law
Categories of Data Subjects	Consumer End Users of Customer's application who interact with the b.well Branded Experience
Categories of	Identity data (name, date of birth, contact information, government-issued

Personal Data	ID for IAL2 verification) Health records and clinical data retrieved through consumer-mediated access Bailey™ Interaction Data (queries, responses, metadata) Usage and tracking data generated through interaction with the b.well Platform Account credentials and authentication data
Special / Sensitive Data	Health data (including PHI as applicable under HIPAA). b.well will apply heightened safeguards consistent with HIPAA requirements and its Business Associate obligations where applicable.
Retention	Personal Data is retained for the duration of the Agreement and deleted or returned within thirty (30) days of termination, subject to legal hold obligations and the archival exception in Section 7 of this DPA.
Transfer mechanisms	Personal Data processed in the United States. Cross-border transfers, if any, subject to Standard Contractual Clauses or other lawful transfer mechanism as required.

DPA Definitions

The following terms, used in this DPA, supplement the definitions in Exhibit A of the Agreement:

"Applicable Data Protection Law" means all applicable data privacy, data protection, and information security laws and regulations governing the Processing of Personal Data by a Party, including without limitation: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations; applicable U.S. state consumer privacy laws (including the California Consumer Privacy Act, as amended, and equivalent state statutes); and any other laws applicable to the Processing of health data or personal data in the jurisdictions in which Customer operates.

"Data Subject" means an individual to whom Personal Data relates, including Consumer End Users.

"Personal Data" means any information that identifies or could be used to directly or indirectly identify, describe, contact, locate, or otherwise relate to or be associated with an individual or household, as defined under Applicable Data Protection Law. For purposes of this DPA, Personal Data includes Protected Health Information (PHI) where b.well acts as a HIPAA Business Associate.

“Processing / Process / Processed” means any operation or set of operations performed on Personal Data, including collection, recording, storage, use, access, disclosure, transmission, alteration, combination, restriction, deletion, or destruction, whether by manual or automated means.

“Security Incident” means any confirmed unauthorized access, disclosure, use, loss, alteration, or destruction of Personal Data Processed by b.well on Customer’s behalf.

“Subprocessor” means any Affiliate or third party engaged by b.well to Process Personal Data on Customer’s behalf in connection with the delivery of the Services.

