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

health.network Acceptable Use Policy

This Acceptable Use Policy ("AUP" or "Policy") governs how Customers may use the b.well Branded Experience and health.network Products and Services. It is incorporated by reference into the health.network Startup Terms of Service (the "Agreement") and has the same legal effect as the Agreement. Terms not defined here have the meanings assigned in the Agreement (including Exhibit A — Definitions) or the Data Processing Addendum (DPA).

In the event of any conflict between this Policy and the Agreement, the Agreement controls unless expressly stated otherwise herein.

b.well's mission is to empower individuals to manage their health through connected, transparent, and trustworthy digital experiences. This Policy reflects b.well's commitment to maintaining the integrity, safety, and reputation of its platform across all Customer integrations. Customers who fail to comply with this Policy are in material breach of the Agreement.

1. Compliance with Applicable Law

Customer must use and present the b.well Branded Experience solely in compliance with all Applicable Law. Customer must not use the b.well Branded Experience in any manner that: (a) violates Applicable Law; or (b) would require b.well to violate Applicable Law as a result of Customer's use or integration.

1.1 Healthcare Regulatory Requirements

Without limiting the foregoing, Customer must:

- comply with HIPAA and its implementing regulations to the extent applicable to Customer's use of the b.well Branded Experience, including requirements applicable to covered entities and business associates;
- comply with applicable state consumer health data privacy laws in all jurisdictions where Customer operates or serves Consumer End Users;
- ensure that all required notices, authorizations, and consent disclosures are provided to Consumer End Users before they use the b.well Branded Experience; and
- not use the b.well Branded Experience in connection with any activity that Customer knows or reasonably should know violates applicable healthcare fraud and abuse laws, including anti-kickback statutes.

1.2 Data Obligations

Customer's data-related obligations under this Policy are consistent with its obligations under the Agreement (Section 3 and Section 6) and the DPA. In particular:

- Customer must store all user data collected through the b.well Platform exclusively within the b.well platform infrastructure, and must not route or replicate that data to external systems without b.well's prior written consent.
- Customer must provide b.well with all user tracking data necessary for b.well's platform analytics and improvement, as described in ToS Section 3.
- Customer must not circumvent, disable, or interfere with any b.well consent mechanism, privacy notice, or data rights workflow required under the Agreement, the DPA, or Applicable Law.

1.3 Regulatory Cooperation

Customer must promptly notify b.well of any governmental or regulatory inquiry, investigation, or proceeding relating to Customer's use of the b.well Branded Experience and must reasonably cooperate with b.well in responding.

2. Brand Integrity and Presentation

b.well's branded experience carries an implicit representation of quality and trustworthiness to Consumer End Users. Customer must not present or deploy it in any way that undermines that trust.

2.1 Branding Requirements

Customer must:

- display b.well's name and Marks prominently within all applications and communications where the Products and Services are used, consistent with ToS Section 3 and Section 10 (Publicity and Brand);
- comply with b.well's then-current brand guidelines, integration specifications, and technical documentation ("Brand Guidelines"), as updated by b.well from time to time upon reasonable notice; and
- not frame, present, or contextualize the b.well Branded Experience in any manner that removes, obscures, or disguises its b.well identity or source.

2.2 Prohibited Conduct

Customer must not:

- present the b.well Branded Experience in a manner that is false, misleading, deceptive, or likely to confuse Consumer End Users as to the source, nature, scope, or capabilities of the experience;
- make any representation about b.well's products, services, data practices, or capabilities that is not expressly authorized in writing by b.well or that is inconsistent with b.well's published documentation;
- alter, modify, obscure, remove, or override any b.well branding, Marks, disclaimers, notices, or consent mechanisms embedded in or required to accompany the b.well Branded Experience;
- present the b.well Branded Experience alongside or within content that is defamatory, obscene, hateful, discriminatory, or otherwise objectionable in b.well's reasonable determination;
- represent or imply that Customer's products are endorsed, certified, sponsored, or provided by b.well, except to the extent expressly authorized in the Agreement; or
- make comparative or superlative claims about the b.well Branded Experience without b.well's prior written consent.

3. Security and Technical Integrity

b.well's platform handles sensitive personal health information. Customer's technical conduct must not introduce or amplify security vulnerabilities that could harm Consumer End Users, b.well, or the broader health data ecosystem.

Customer must not:

- attempt to probe, scan, penetration test, or test the vulnerability of b.well's systems, networks, or infrastructure without b.well's prior written authorization;
- introduce, transmit, or facilitate the transmission of any malicious code, virus, worm, ransomware, or other harmful component through or in connection with the b.well Branded Experience;
- interfere with, disrupt, or degrade the integrity, availability, performance, or security of b.well's systems, services, APIs, or data;
- attempt to reverse engineer, decompile, disassemble, or derive the source code or algorithms of any b.well component, except to the limited extent expressly permitted by Applicable Law;
- circumvent, disable, or interfere with any access control, authentication mechanism, rate limit, or security feature of the b.well Branded Experience or related APIs;
- deploy the b.well Branded Experience in a technical configuration not authorized by b.well's documentation that could reasonably be expected to introduce security risks; or
- collect, transmit, store, or process data through the b.well Branded Experience in a manner that violates b.well's security requirements or the DPA.

Customer must maintain industry-standard security controls for its own systems and integration environment, including appropriate access controls, encryption in transit and at rest, and vulnerability management practices. Customer must notify b.well's security team in writing within forty-eight (48) hours of becoming aware of any actual or suspected Security Incident involving the b.well Branded Experience, b.well data, or Consumer End User data processed through the integration.

4. Other Prohibited Uses

Customer must not use the b.well Branded Experience:

- in connection with any activity that is illegal, fraudulent, harmful to third parties, or that encourages Consumer End Users to engage in any conduct that violates this Policy;
- to generate disproportionate, excessive, or abusive automated traffic or API queries on b.well's infrastructure beyond any usage parameters in the Agreement;

- in a manner intended or reasonably likely to harm b.well's goodwill, trade reputation, or relationships with its regulators, partners, or other customers;
- in connection with any product, service, or campaign that directly competes with b.well's core product offerings, unless expressly authorized; or
- in any manner that would subject b.well to regulatory action, negative press coverage, or third-party claims arising from Customer's conduct.

Customer must promptly notify b.well of any circumstance Customer becomes aware of that is reasonably likely to result in harm to b.well's business, reputation, or legal standing arising from Customer's integration or use of the b.well Branded Experience.

5. Monitoring and Audit

b.well reserves the right to monitor Customer's integration for compliance with this Policy using technical means, including API usage monitoring, logging, and anomaly detection, consistent with the Agreement and Applicable Law.

Upon reasonable prior written notice of no less than ten (10) business days (except in the case of a suspected material breach or Security Incident), b.well may audit Customer's use of the b.well Branded Experience to verify compliance with this Policy, no more than once per calendar year absent a specific compliance concern. Audits will be conducted in a manner that minimizes disruption to Customer's operations. Customer will cooperate reasonably and provide b.well with reasonable access to relevant records, personnel, and systems.

Customer will conduct periodic internal reviews of its integration to confirm compliance with this Policy and will promptly notify b.well in writing of any known or suspected violation.

6. Enforcement and Remedies

A violation of this Policy is a material breach of the Agreement. b.well's remedies set out below are in addition to all other remedies available at law or in equity.

6.1 Immediate Suspension

b.well may suspend Customer's access to the b.well Branded Experience immediately and without prior notice in the event of:

- a material or ongoing violation of this Policy that poses an imminent risk of harm to Consumer End Users, b.well, or third parties;

- an active or suspected Security Incident involving the integration; or
- a regulatory or legal requirement to suspend access.

6.2 Cure Period for Non-Emergency Violations

For violations that do not pose an imminent risk of harm, b.well will provide Customer with written notice and a cure period of fifteen (15) calendar days to remediate. If Customer fails to cure within that period, b.well may suspend or terminate Customer's access in accordance with the Agreement.

6.3 Termination

Repeated, willful, or uncured material violations of this Policy constitute grounds for termination of the Agreement in accordance with its terms. Upon termination, Customer's wind-down obligations under Order Form Section 5 (Term, Renewal, and Termination) apply immediately.

6.4 Indemnification

Customer's indemnification obligations under ToS Section 9 expressly cover claims arising from Customer's breach of this Policy, Customer's violation of Applicable Law in connection with its integration, and any misrepresentation by Customer to Consumer End Users regarding the b.well Branded Experience.

7. Updates to This Policy

b.well may update this Policy from time to time to reflect changes in its products, Applicable Law, or industry standards. Updates are effective upon posting at icanbwell.com/legal/health-network-startup-acceptable-use-policy/. Customer's continued use of the b.well Branded Experience following the effective date of any update constitutes acceptance. If Customer objects to any material change, Customer may terminate the Agreement in accordance with its terms upon thirty (30) days' written notice.

8. Contact

Questions about this Policy, requests for authorization, or reports of known or suspected violations should be directed to:
b.well Connected Health, Inc.
Legal & Compliance Email: legal@bwell.com
Address: 145 West Ostend Street, Suite 300, Baltimore MD 21230

For security incidents, contact b.well's security team directly at security@bwell.com within forty-eight (48) hours of discovery, as required by DPA Section 3.2.

By accepting the Agreement that incorporates this Policy, Customer acknowledges that it has read, understood, and agrees to comply with this Acceptable Use Policy in its entirety.

