Washington Consumer Health Data Privacy Policy

Effective Date: October 19, 2026

Last Updated: October 19, 2026

Entity: Pacific Northwest Kaizen, PLLC, doing business as **Doc Bee Well** ("Doc Bee Well," "we," "us," or "our")

Published Policy & Request Page: Washington Health Privacy

At Doc Bee Well, we believe your health and wellness information belongs to you. Pacific Northwest Kaizen, PLLC operates **Doc Bee Well** (which provides direct-pay primary care, telehealth, laboratory services, and Honey Bee membership services) and the **You Bee Well** wellness application.

This **Washington Consumer Health Data Privacy Policy** ("Consumer Health Policy") explains how we collect, use, disclose, and protect **non-exempt Consumer Health Data** governed by Washington's My Health My Data Act (Chapter 19.373 RCW) ("MHMDA"). It also transparently distinguishes between privacy controls verified in our accepted software implementation and administrative or technical procedures that are currently undergoing final production verification.

1. How This Policy Relates to Our Other Privacy Notices & Healthcare Exemptions

Because Doc Bee Well provides both **clinical medical care** and **consumer-directed wellness and digital services**, different privacy laws apply depending on the **origin, purpose, and handling** of your information. Under RCW 19.373.100, clinical healthcare information is exempt from the My Health My Data Act when it is collected, used, or disclosed in accordance with federal HIPAA rules or Washington's Uniform Health Care Information Act (Chapter 70.02 RCW).

To provide clear, non-duplicative disclosures, we maintain three distinct privacy notices:

Privacy Notice	Information Covered	Governing Law
1. This Washington Consumer Health Data Privacy Policy	**Non-Exempt Consumer Health Data:** Self-directed wellness measurements, goals, check-ins, and non-clinical coaching records in *You Bee Well*; prospective-patient inquiries, pre-clinical chats, and pre-purchase laboratory browsing before clinical care attaches; and health-related website or conversion telemetry that is not exempt clinical healthcare information.	Washington My Health My Data Act (**Chapter 19.373 RCW**)
2. Doc Bee Well HIPAA Notice of Privacy Practices (NPP) / Healthcare Information Notice	**Exempt Clinical Healthcare Information:** Information identifying a patient that directly relates to clinical healthcare provided by a licensed healthcare provider to diagnose, treat, or maintain a physical or mental condition—including clinical scheduling, patient intake records, clinical telehealth/visit records, ordered laboratory tests and results, physician-directed wellness monitoring, and records intermingled within our clinical record system.	Federal **HIPAA** (45 C.F.R. Parts 160 & 164) and Washington **Chapter 70.02 RCW** (exempted from MHMDA under **RCW 19.373.100(1)(a)(i)–(ii) and (1)(b)**)

Privacy Notice	Information Covered	Governing Law
3. General Website & *You Bee Well* Privacy Policy	**Non-Health Administrative, Financial & Security Data:** Ordinary account authentication credentials, payment processing tokens decoupled from health status, basic network routing logs, and de-identified/non-linkable aggregate operational data.	General Federal and State Privacy and Consumer Protection Laws

How Healthcare Exemptions Apply Across Doc Bee Well & *You Bee Well* (RCW 19.373.100(1))

1. **Ordinary Healthcare-Information Exemption (RCW 19.373.100(1)(a)(i)–(ii)):** Information collected, used, or disclosed to provide clinical diagnosis, treatment, or health maintenance by a Doc Bee Well healthcare provider under Chapter 70.02 RCW or HIPAA is exempt from MHMDA—regardless of whether it is stored in our Electronic Health Record (EHR) or a dedicated clinical database.
2. **Intermingled Healthcare Records Exemption (RCW 19.373.100(1)(b)):** Information originating from, and intermingled to be indistinguishable with, exempt HIPAA or Chapter 70.02 RCW clinical records maintained by Doc Bee Well as a healthcare provider is also exempt from MHMDA.
3. **Why Database Location Alone Does Not Create an Exemption:** Housing information in a separate *You Bee Well* database does not automatically make it exempt or non-exempt. Instead, when you use *You Bee Well* for **self-directed personal wellness** outside of a physician-directed clinical treatment plan, or when you interact with public website pages before becoming a clinical patient, that information is treated as **non-exempt Consumer Health Data** covered by this policy.

2. Categories of Non-Exempt Consumer Health Data We Collect

Depending on how you interact with Doc Bee Well and *You Bee Well*, we collect—or our systems are architected to process—the following six categories of non-exempt (or hybrid) Consumer Health Data:

Category 1: Personal Health Measurements & Connected-Device Data

- **Server Manual Wellness Observations & Transferred Local Measurements:** Metric names, values, units, measurement timestamps/time zones, source provenance, and revision/correction lineage when you manually log observations on our server or explicitly transfer selected local measurements from your phone.
- **Explicitly Synchronized Health Connect Measurements:**
    - *Steps:* Step counts, intervals/aggregates, source origin (such as Health Connect or Samsung-origin records), and time provenance when you explicitly initiate synchronization to your *You Bee Well* server ledger.
    - *Heart Rate:* Beats-per-minute (BPM) samples, timestamps/intervals, source provenance, and sync receipts when you grant Android category permission and explicitly initiate category synchronization.
    - *Canonical Synchronized Measurement History:* Selected measurement values/samples, units, source IDs, start/end timestamps, time-zone offsets, and cryptographically signed transfer receipts stored in your server measurement history.
- **Unactivated Development Categories:** While our underlying development code includes data structures for additional Health Connect categories (weight, height, body fat, basal metabolic rate, blood pressure, blood glucose, oxygen saturation, sleep, exercise, nutrition, distance, calories, power, speed, and VO2 max), **release permissions are not declared for these categories in our production release manifest**, and they are not collected by our server unless separately approved, enabled, and authorized in a future release.

Category 2: Wellness Goals, Check-Ins & Reflections

- **Server Goals and Check-Ins:** Goal titles, personal reasons, target frequencies, goal status, daily check-in outcomes, free-text progress notes, and revision history stored on our server.
- **Phone-Only Reflections & Untransferred Local Wellness Entries:** Private reflection notes (bounded to 180 entries / 1,000 characters) and offline local wellness entries (up to 2,000 events) stored in your Android device's local application storage. **Important:** Phone-only reflections have no server sync or export path and are never transmitted to Doc Bee Well servers. Local wellness entries remain solely on your phone unless you explicitly select and activate a transfer to your online account.

Category 3: Wellness Coaching & Pathway Records

- **Coaching Assignments and Entries:** Coaching assignment labels/keys, coaching notes, encouragement and action items, next check-in schedules, and scoped coach views of your goals and check-ins when participating in non-clinical wellness coaching. (If coaching is provided as part of clinical care under Chapter 70.02 RCW, those clinical records are governed by our HIPAA/Healthcare Notice).

Category 4: Prospective-Patient, Pre-Clinical & Service-Seeking Interactions

Under RCW 19.373.010(8)(b)(xii), Consumer Health Data includes information that identifies a consumer as **seeking healthcare services**. While clinical records for established patients are exempt under Chapter 70.02 RCW and HIPAA, the following information may contain non-exempt Consumer Health Data when created by prospective patients, website visitors, or members outside of clinical care:

- **Pre-Clinical Nurse Bee Conversations:** Chat messages, user-supplied context, conversation IDs, timestamps, and safety/red-flag routing statuses when a website visitor or prospective patient interacts with our Nurse Bee conversational assistant prior to clinical care, or requests an email summary.
- **Pre-Patient Scheduling, Intake & Membership Inquiries:** Contact details, requested visit types/times, pre-visit clinical intake answers and acknowledgments, Honey Bee membership enrollment applications and contact consents, and optional Honey Bee member update preferences to the extent collected or retained

for prospective-patient outreach or non-clinical wellness administration rather than exempt Chapter 70.02 RCW clinical charting.

- **Pre-Purchase Lab Marketplace Activity & Health-Linked Payment Metadata:** Selections of laboratory test products, checkout status, and Stripe payment/checkout descriptions or reference metadata to the extent they link your identity to specific health tests sought outside of an exempt clinical record.
- **Health-Linked Email & SMS Communications:** Transactional notices or separately opted-in communications sent via Microsoft 365 or RingCentral when linked to non-exempt wellness services or prospective-patient inquiries.

Category 5: Public Website, Analytics & Advertising Telemetry

- **Public Website Activity & Third-Party Scripts:** When you visit our public website (docbeewell.com, hosted via GoDaddy), browser/cookie identifiers, IP addresses, URL/referrer paths, and form interactions may be collected. Our October 16, 2026 technical audit confirmed that the public docbeewell.com website includes **Google Tag Manager (GTM), Google Analytics, Google Ads conversion tracking (including an inspected laboratory-readiness conversion trigger in GTM), Meta Pixel, and GoDaddy website analytics/performance scripts**. While our audit did not establish whether the laboratory-readiness trigger actively fires during patient interactions, any pairing of persistent browser/advertising identifiers with pages or actions indicating that you are seeking specific healthcare or laboratory services may constitute Consumer Health Data under Washington law.
- **First-Party Analytics, Conversion Outbox & External Projections:** Within our separate protected application environment, our software logs first-party client/session/click identifiers, funnel events, and conversion outbox records. Although code exists for external Google Analytics 4 (GA4) and Google Ads projections, browser-side Google tracking is disabled (false) in the inspected application UI, and server-side external delivery is held behind administrative enable/dry-run gates.
- **Internal Advertising Advisor Aggregates:** Validated aggregate advertising snapshots processed for internal marketing analysis (using an OpenAI Responses adapter when enabled). This dataset does not include individual chat transcripts, though we disclose it here because formal statistical de-identification certification has not been separately established.

Category 6: *You Bee Well* Account, Device & Privacy Administration Records

When linked to your *You Bee Well* health profile, technical and administrative records that manage your wellness account may be associated with Consumer Health Data:

- **Member Participation, Authentication & Device Binding:** Principal-subject participation mappings, member authentication and account recovery logs, and cryptographic device registration records, public-key fingerprints, and pairing challenges used to authorize device data transfers.
- **Consent History, Privacy Requests & Security Audit Logs:** Immutable metric-sharing consent epochs and signed transfer receipts, logged privacy/deletion requests, and least-privilege security/operational audit logs.

3. Sources of Consumer Health Data

We collect non-exempt Consumer Health Data from the following sources:

1. **Directly from You:** When you enter wellness observations, goals, check-ins, Nurse Bee chat messages, membership applications, lab selections, or appointment requests.
2. **Your Mobile Device & Android Health Connect (Upon Explicit Action):** When you grant Android operating-system permissions and take explicit action within *You Bee Well* to transfer local measurements, synchronize Steps, or synchronize Heart Rate from your registered device.
3. **Your Browser, Device & Network Connections:** Automatically captured IP addresses, URL/referrer headers, device signatures, and—on our public GoDaddy-hosted website (docbeewell.com)—cookies or script telemetry from GoDaddy, Google Tag Manager/Analytics/Ads, and Meta Pixel.
4. **Authorized Staff, Coaches & Service Workflows:** Coaching notes or assignment updates entered by an authorized wellness coach and operational status updates recorded by authorized Doc Bee Well personnel.

4. Purposes for Collecting and Using Consumer Health Data

We collect and use non-exempt Consumer Health Data for the following specific purposes:

Purpose of Collection & Use	Legal Basis Under RCW 19.373.030
1. Providing Requested *You Bee Well* Wellness, Sync & Coaching Services: Maintaining your personal wellness history, synchronizing selected Health Connect Steps and Heart Rate metrics from your registered device, tracking your wellness goals and check-ins, and delivering assigned wellness coaching.	Necessary to provide a product or service you requested (**RCW 19.373.030(1)(a)(ii)**) and/or your affirmative opt-in consent per metric category (**RCW 19.373.030(1)(a)(i)**).
2. Responding to Pre-Clinical Inquiries, Scheduling, Lab Orders & Memberships: Assisting visitors via Nurse Bee chat, scheduling requested appointments, processing Honey Bee membership applications and optional member updates, and fulfilling laboratory test selections and payments.	Necessary to provide a service you requested (**RCW 19.373.030(1)(a)(ii)**) or your separate opt-in for optional updates.
3. Account Security, Cryptographic Device Pairing & Consent Enforcement: Authenticating members, verifying cryptographic device signatures before accepting measurement uploads, logging consent epochs and privacy requests, and preventing unauthorized access or fraud.	Necessary to provide the requested service and statutory security/integrity operations (**RCW 19.373.100(3)**).
4. Website Delivery, Funnel Measurement & Advertising Attribution Review: Operating our public website, reconciling first-party conversion events, and reviewing aggregate marketing performance. *(See Section 5 regarding our active review and minimization of public website third-party scripts).*	Site delivery necessity; third-party advertising/analytics telemetry is currently under technical remediation and restriction review.

5. How We Disclose or Share Consumer Health Data & Categories of Recipients

A. Corporate Affiliates

None. Pacific Northwest Kaizen, PLLC operates Doc Bee Well and *You Bee Well* directly and has **no corporate affiliates** (parent, subsidiary, or sibling corporate entities) that receive Consumer Health Data.

B. Contracted Processors (Service Providers)

Doc Bee Well's operational policy is to strictly limit external disclosures of your information to contracted **Processors** (service providers that process data on our behalf to support the services you request). Depending on the workflow you use, our infrastructure and communications processors include:

- **Cloud & Network Infrastructure: Cloudflare** (which routes and protects traffic to Doc Bee Well origin servers per our network architecture) and **GoDaddy** (which hosts our public informational website docbeewell.com).
- **Communications & Productivity Providers: Microsoft 365** (for transactional email notices, requested Nurse Bee email summaries, and optional Honey Bee updates) and **RingCentral** (for SMS and telecommunications support).
- **Payment Processing: Stripe** (when you complete a payment or checkout transaction for laboratory testing, appointments, or memberships).
- **AI & Analytical Processing:** Local/internal language models (such as **Ollama** for intake translation and local Nurse Bee routing) and, solely for aggregated internal advertising snapshots, **OpenAI** (when enabled).

Note on Processor Contracts: Under RCW 19.373.060, Processors must be bound by written contracts limiting their processing to our instructions. We are actively verifying edge logging configurations and completing MHMDA-specific processor addenda across our infrastructure providers.

C. Current Status of Public Website Third-Party Advertising & Analytics Scripts

We do not sell your Consumer Health Data for monetary consideration, and within our protected patient/member application UI, browser-side Google tracking is disabled (false).

However, our October 16, 2026 technical audit identified that our **public website (docbeewell.com)** currently loads third-party scripts from **Google (Google Tag Manager, Google Analytics, Google Ads conversion tracking, including an inspected laboratory-readiness trigger)** and **Meta (Meta Pixel)**, in addition to **GoDaddy website analytics**.

- **Categories Potentially Transmitted on the Public Website:** If these scripts fire while you browse health-related pages or initiate a laboratory/appointment action on docbeewell.com, browser headers, IP addresses, cookie/advertising IDs, and page URL/event parameters may be transmitted to **Google, Meta, or GoDaddy**.
- **Our Remediation & Consent Posture:** Under Washington law, transmitting linkable Consumer Health Data to third-party advertising platforms outside of strict processor contracts requires separate, unbundled opt-in sharing consent (RCW 19.373.030(2)) or a valid sale authorization (RCW 19.373.070). We do not represent that a website cookie banner currently satisfies MHMDA sharing consent, nor do we claim that public website pages are currently free of third-party script requests. Instead, we are actively auditing and minimizing or disabling third-party advertising triggers on health-related pages and verifying final Android network behavior prior to public Google Play release.

6. How Consent and Withdrawal Work in *You Bee Well*

A. Collection Consent vs. Local Device Permissions

You Bee Well separates **local Android operating-system permissions** from **explicit authorization to synchronize** health data to Doc Bee Well's servers:

- Granting Android Health Connect permission (READ_STEPS or READ_HEART_RATE) allows local preview on your phone but **does not** automatically upload your data to our servers.
- Server collection occurs only after you complete cryptographic device pairing, grant category sharing authorization, and initiate an explicit sync action.

B. Verified Controls to Withdraw Consent & Stop Future Synchronization

In the accepted Android development implementation and Owner-installed APK of *You Bee Well* (note: these controls have been verified in our accepted development build and Owner-installed APK, and have not yet been verified as publicly available through Google Play), you can withdraw consent and stop future collection using the following exact controls:

1. **Withdraw Heart Rate Sharing Authorization:**
    - **Path:** You Bee Well → Settings → Open Category sharing & permissions → Heart rate → Disconnect sharing with Wellness

- **Effect:** Immediately withdraws your authorization for future Heart Rate sharing with your online Wellness account.

2. **Stop Future Steps Synchronization:**
    - **How Steps Sync Works:** Steps synchronization is off by default and requires an explicit manual action through Wellness → Your Daily Movement → Sync to You Bee Well.
    - **How to Stop Future Access:** There is currently no separate Steps-specific sharing-withdrawal button in the app. You can stop any future Steps access at any time by revoking the Steps permission in Android Health Connect (see Step 4 below) or by disconnecting your registered device (see Step 3 below).
3. **Disconnect a Registered Device (Revoke Server Authorization):**
    - **In-App Path:** You Bee Well → Settings → Manage device connection → Disconnect device (Displays confirmation: *"Disconnected; server revocation confirmed."*)
    - **Web Portal Path:** Authenticated members can also visit **https://wellness.docbeewell.com/you-bee-well/devices** and select Your connected devices → Disconnect device.
    - **Effect:** Immediately revokes that device's cryptographic server authorization so it can no longer upload measurements.
4. **Withdraw Android Health Connect Permissions:**
    - **Path from *You Bee Well*:** Settings → Open Category sharing & permissions → Heart rate → Review Android permission settings
    - **Inside Android Health Connect:** Navigate to App permissions → You Bee Well and disable the **Steps** or **Heart Rate** permissions (exact Android menu labels may vary by device and OS version).
    - **Effect:** Prevents the *You Bee Well* app on your phone from reading any further data from Health Connect.

C. Important Distinctions Regarding Withdrawal Controls

- **There is no global "Disable Cloud Sync" toggle** and no separate Steps-specific sharing-withdrawal button; instead, withdrawal is managed through the specific category, device-disconnection, and Android permission controls listed above.

- **Withdrawing Consent Stops Future Collection Only:** Revoking Android permissions, disconnecting Heart Rate sharing, or disconnecting a registered device immediately stops **future** data access or server uploads, but **none of these actions automatically deletes measurements that were previously synchronized to your online Wellness account**. To request deletion of previously synchronized server data, please see Section 7 below.

7. Your Rights to Access, Delete & Appeal (And Current Operational Status)

Under Chapter 19.373 RCW, Washington consumers have the right to confirm and access their non-exempt Consumer Health Data, withdraw consent, request deletion, and appeal a refusal to act on a request.

A. Right to Confirm and Access (RCW 19.373.040(1)(a))

You may request confirmation of whether we collect, share, or sell your Consumer Health Data and request access to that data (including a list of any third parties or affiliates with whom it was shared and their contact mechanisms) free of charge up to twice per year.

B. Right to Delete & Current Implementation Status

You have the statutory right under RCW 19.373.040(1)(c) to request the deletion of your non-exempt Consumer Health Data.

Important Transparency Disclosure on Current Deletion Capabilities:

- **Local Phone Data:** You can delete local-only reflections and offline local wellness entries immediately on your phone using the app's local clear controls.
- **Server-Side Synchronized Data & Active Verification Status:** In our current server architecture, synchronized wellness observations, goals/check-ins, coaching entries, Steps ledgers, and measurement histories are stored in append-only database tables, and our privacy-request tracking service records deletion requests for human administrator review but **does not yet have a verified automated server-side deletion executor**.
- **How We Handle Deletion Requests During Verification:** Until our automated end-to-end deletion executor across active database tables, downstream processors, and backup archives is independently verified, when you submit a deletion request:
    1. We will log and authenticate your request and help you revoke active device and category sync authorizations so no additional data is uploaded;

2. Our administrator team will review your request to separate non-exempt Consumer Health Data from exempt clinical medical records that we are legally required to retain under Chapter 70.02 RCW; and
3. We will coordinate manual record removal across our active non-exempt database tables and applicable processors, and manage archived/backup copies in accordance with RCW 19.373.040(2)(b) (which permits delayed deletion on backup systems for up to **six (6) months** after authentication unless earlier restored or accessed for a commercial purpose).

8. How to Submit a Privacy Request or Appeal

A. Submitting an Access, Withdrawal, or Deletion Request

You may submit a request free of charge through any of the following channels:

- **Email: admin@docbeewell.com** (Please include *"Washington Consumer Health Data Request"* in the subject line).
- **U.S. Mail:**

Pacific Northwest Kaizen, PLLC (d/b/a Doc Bee Well)

Attn: Privacy Officer

1201 Pacific Ave, Suite 646

Tacoma, WA 98402

Response Timeline: We will authenticate your request using commercially reasonable efforts and respond within **45 days** of receipt (extendable once by an additional 45 days when reasonably necessary, provided we notify you within the initial 45-day period).

B. How to Appeal a Refusal (RCW 19.373.040(7))

If we decline to take action on your request (for example, if the requested information is exempt clinical healthcare information governed by Chapter 70.02 RCW or HIPAA), we will notify you within 45 days with the reasons for our decision.

- **Submitting an Appeal:** You may appeal our decision by emailing **admin@docbeewell.com** with the subject line *"MHMDA Privacy Appeal"* or writing to our Tacoma mailing address above.

- **Appeal Decision & Washington Attorney General Complaint Link:** Within **45 days** of receiving your appeal, we will inform you in writing of any action taken or not taken and our reasons. If your appeal is denied, our written notice will provide instructions for contacting the **Washington State Office of the Attorney General** to submit a complaint, which you may do online at **https://www.atg.wa.gov/file-complaint**.

9. Internal Access Controls, Processor Duties & Geofencing

- **Restricted Access (RCW 19.373.050):** We restrict internal access to non-exempt Consumer Health Data to authorized personnel and service workflows for whom access is necessary to provide the service you requested (such as scoped member access and explicitly assigned coaches, rather than unrestricted staff access)[cite: 1].
- **Geofencing Prohibition (RCW 19.373.080):** Doc Bee Well and *You Bee Well* do not use geofences (virtual perimeters within 2,000 feet of in-person healthcare facilities) to track consumers, collect Consumer Health Data, or send health-related notifications or advertisements.