



BOWER HOUSE — PRIVACY POLICY

Bower House Holdings, LLC

Effective Date: June 16, 2026

1. INTRODUCTION

This Privacy Policy explains how Bower House Holdings, LLC ("Bower House," "we," "us," or "our") collects, uses, discloses, and protects personal information in connection with the Bower House Club App, the Bower House website located at bowerhouse.com (the "Website"), and all related software, features, content, communications, and services (collectively, the "Services"). By using the Services, you acknowledge this Privacy Policy. This Privacy Policy should be read together with our Terms of Service, which are incorporated by reference.

2. RELATIONSHIP TO HIPAA AND YOUR HEALTH RECORD

Bower House operates as a hybrid entity for purposes of the federal Health Insurance Portability and Accountability Act (HIPAA). Protected Health Information that we create or receive in connection with research or clinical services is governed by our Notice of Privacy Practices and by the HIPAA authorizations you sign, and not by this Privacy Policy. This Privacy Policy governs the consumer personal information we collect through the Services that is not Protected Health Information. Where a feature of the Services handles Protected Health Information, the applicable HIPAA notices and authorizations control. If you are a research participant who has signed separate informed consent and HIPAA authorization documents, those documents govern the use and disclosure of your health information for research purposes.

3. INFORMATION WE COLLECT

We collect the following categories of personal information:

- **Identifiers and account information:** name, email address, telephone number, username, and account credentials.
- **Health and wellness data:** We collect health and wellness data through multiple pathways, including:

Device and platform integrations: data you choose to share through wearable devices, Apple Health / HealthKit, Android Health Connect, and Fitbit and Garmin accounts you authorize, including activity, sleep, heart rate, and related wellness metrics. Note: the Oura Cloud API integration is not currently active; Oura data reaches the Services only through Apple Health exports and legacy imports. Fitbit and Garmin connections exist but data synchronization is not currently active.

Electronic health record imports: patient-exported records from Epic MyChart (ZIP upload), FHIR bundle JSON uploads, and Apple Health clinical records, including labs, medications, conditions, immunizations, procedures, and insurance coverage records. Note: this is not a live connection to your healthcare provider's systems; data enters the Services only through patient-initiated export and upload.

Practitioner-entered data: health metrics and clinical data entered directly by your care provider through the practitioner web application, including body composition scan values (such as InBody results), free-text lab entries, ECG recordings (including raw voltage waveform data), and clinical records such as encounters, conditions, surgeries, allergies, and medications.

Document uploads: PDFs, images, and clinical documents (including imaging and diagnostic reports) that you or your care provider upload, up to 50 MB per file. Uploaded documents are stored securely and may be processed using optical character recognition (OCR) technology to extract health information such as lab values, medications, and diagnoses, which may then be stored as part of your health record.

Lab result imports: lab results from Function Health and Quest Diagnostics, imported as PDFs from in-person phlebotomy services.

Legacy health file imports: data imported through the Bower House Master Health File format, including labs, protocol logs, wearable metrics, and body composition data.

AI-assisted health fact extraction: health information detected in free-text communications within the Services may be identified using automated tools and, upon review and acceptance by your care provider, written into your health record.

All health and wellness data described above is treated as sensitive personal information and, to the extent it constitutes Protected Health Information, is governed by the HIPAA documents referenced in Section 2.

- **Usage and device information:** interactions with the Services, features used, device identifiers, operating system, log data, and diagnostics.
- **Location information:** approximate location derived from your IP address. The App does not request location permissions and does not collect real-time or precise GPS location from your device. The only location data that may be present in the Services is historical GPS route information contained within a health-data export file that you choose to import (for example, workout routes within an Apple Health export). Such data is used solely to display workout route and distance information and is not used for advertising, geofencing, or any other location-based purpose.
- **Communications:** messages, support requests, and feedback you send through the Services.
- **User Content:** content you submit, upload, or transmit through the Services, as described in the Terms of Service.
- **Inferences:** inferences drawn from the categories above to create a profile reflecting your preferences, characteristics, or behavior within the Services.
- **Sensitive personal information:** certain information described above may constitute "sensitive personal information" under California law or comparable categories under other state privacy laws, including health and wellness data, precise geolocation, and account log-in credentials. We process sensitive personal information only as necessary to provide the Services and for other purposes permitted by law. We do not use or disclose sensitive personal information to infer characteristics about you for purposes of advertising. (Note: Face ID and Touch ID authentication is performed entirely by your device's

operating system. Bower House does not receive, access, or store any biometric data from these processes.)

4. SOURCES OF INFORMATION

We collect personal information from the following sources: (a) directly from you, such as when you create an account, make a purchase, submit User Content, or contact us; (b) automatically through your use of the Services, such as usage data, device information, and approximate location; (c) from third-party sources you authorize, such as connected devices, Apple Health / HealthKit, and electronic health record platforms; (d) from our payment processor, Square, Inc., which provides us with transactional data such as transaction amount, date, status, and payment method type in connection with purchases you make through the Services; and (e) from our other service providers, such as analytics providers, to the extent they return information to us in connection with the services they perform on our behalf.

5. HOW WE USE INFORMATION

We use personal information for the following purposes: to provide, operate, maintain, and improve the Services and their features; to create and manage your account; to process transactions, subscriptions, and membership fees; to deliver and personalize wellness content, recommendations, and features; to communicate with you, including service messages, transactional messages, and, where you opt in, promotional communications and text messages; to respond to your inquiries and support requests; to conduct analytics and internal research to understand how the Services are used and to improve our offerings; to maintain the security and integrity of the Services and to detect and prevent fraud; to enforce our Terms of Service; and to comply with legal obligations. Where the Services present recommendations generated with the assistance of automated or artificial-intelligence tools, those recommendations are reviewed by a licensed clinician before they are communicated to you. We do not use automated decision-making to produce legal or similarly significant effects concerning you without human review.

6. HEALTH DATA: SPECIAL COMMITMENTS

Health and wellness data you share through HealthKit or comparable platforms is used only to provide you with the Services. We do not use this data for advertising, we do not sell it, we do not share it with data brokers, and we do not disclose it to third parties except to service providers acting on our behalf under contract, as you direct, or as required by law and permitted by the applicable platform rules.

7. HOW WE DISCLOSE INFORMATION

We may disclose personal information to the following categories of recipients and for the following purposes: (a) service providers and contractors who process information on our behalf under written contracts that restrict their use of the information to the services they perform for us; (b) entities within the Bower House Family for the purposes described in this Privacy Policy; (c) professional advisors, including legal counsel, auditors, and consultants, as necessary for their engagement; (d) law enforcement, regulators, courts, and other governmental authorities where required by law, legal process, or to protect the rights, safety, or

property of Bower House, our users, or others; and (e) a potential or actual acquirer, successor, or assignee in connection with a merger, acquisition, financing, reorganization, or sale of assets, in which case the acquiring entity will be bound by this Privacy Policy with respect to personal information transferred, or we will provide you with notice and, where required by law, an opportunity to consent. We do not disclose personal information to third parties for their own independent marketing purposes.

8. WE DO NOT SELL OR SHARE FOR CROSS-CONTEXT BEHAVIORAL ADVERTISING

Bower House does not sell your personal information, and does not share your personal information for cross-context behavioral advertising, as those terms are defined under the California Consumer Privacy Act. We do not use personal information received from third-party sources for purposes of cross-context behavioral advertising. We recognize the Global Privacy Control (GPC) signal. When we detect a GPC signal from your browser or device, we treat it as a valid opt-out request under the California Consumer Privacy Act and process it accordingly.

9. YOUR CALIFORNIA PRIVACY RIGHTS

If you are a California resident, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, provides you with the following rights regarding your personal information:

- Know and access the categories and specific pieces of personal information we have collected about you.
- Delete personal information we have collected from you, subject to legal exceptions.
- Correct inaccurate personal information.
- Opt out of the sale or sharing of personal information. Because we do not sell or share personal information for cross-context behavioral advertising, there is no such activity to opt out of, but we honor opt-out preference signals as described in Section 8.
- Limit the use and disclosure of sensitive personal information. We already restrict our use of sensitive personal information to permitted purposes as described in Section 3.
- Not receive discriminatory treatment for exercising your rights.

To exercise these rights, use the Privacy Choices setting in the App or Website, or email privacy@bowerhouse.com. You may designate an authorized agent to submit a request on your behalf; we may require the agent to provide proof of authorization. We will verify your identity before fulfilling a request, which may require you to confirm information associated with your account. We will respond to verifiable requests within the timeframes required by applicable law (45 days under California law, subject to a permitted extension). If we deny a request in whole or in part, we will explain the basis for the denial. You may appeal a denial by contacting us at privacy@bowerhouse.com with the subject line "Privacy Rights Appeal," and we will respond to your appeal within the timeframe required by applicable law.

10. OTHER STATE PRIVACY RIGHTS

Residents of states with comprehensive privacy laws, including but not limited to Colorado, Connecticut, Virginia, Oregon, Texas, Delaware, Iowa, New Jersey, Tennessee, Indiana, Montana, and Utah, may have rights to: access and obtain a copy of their personal information; delete personal information; correct inaccurate personal information; opt out of targeted advertising, the sale of personal information, or profiling in furtherance of decisions that produce legal or similarly significant effects; and, where applicable, appeal a denial of a privacy rights request. To exercise these rights, contact us using the information in Section 18. We will respond within the timeframes required by the applicable state law.

Additional Disclosures for Nevada Residents

If you are a Nevada resident, Nevada Senate Bill 370 ("Nevada SB 370") provides you with additional rights with respect to consumer health data. Consumer health data, as defined under Nevada law, includes personal information that identifies or is reasonably linkable to a consumer and that is used to identify a consumer's physical or mental health status, including data collected from devices, applications, and platforms that you connect to the Services.

Bower House does not sell consumer health data as that term is defined under Nevada SB 370. We do not exchange consumer health data for monetary or other valuable consideration, and we do not share consumer health data with third parties except as described in Section 7 of this Privacy Policy.

If you are a Nevada resident, you may submit a request to access or delete your consumer health data by using the Privacy Choices setting in the App or on the Website, or by contacting us at privacy@bowerhouse.com. We will verify your identity before fulfilling any such request and will respond within the timeframes required by applicable Nevada law.

To the extent required by Nevada SB 370, we obtain your consent before collecting or sharing consumer health data. You may provide or withdraw consent through the privacy settings available within the Services or by contacting us at privacy@bowerhouse.com. Withdrawal of consent will not affect the lawfulness of any processing conducted prior to your withdrawal.

11. COOKIES AND TRACKING

We use cookies and similar technologies across our Services. The technologies in use differ by surface:

Practitioner web application and consumer mobile app: We use only strictly necessary, first-party cookies and local storage to operate and secure these surfaces. Specifically, we use two first-party session authentication cookies (`access_token` and `refresh_token`) and three local storage keys for user interface preferences. We do not use third-party analytics SDKs, advertising pixels, behavioral-analytics tools, or session-replay technologies on these surfaces.

Marketing website (bowerhouse.com): Our marketing website is hosted on WordPress.com and uses the following technologies operated by Automattic, Inc. and other third parties: Jetpack Stats (a web analytics beacon operated by Automattic); the Blaze advertising module (an Automattic advertising tool); the Photon CDN (an Automattic content delivery network); Google Fonts (operated by Google); Gravatar (an Automattic

avatar service); and a Google Maps embed (which may allow Google to set cookies within the embedded frame). A third-party scroll-animation library is also loaded from unpkg.com. Automattic also receives data as the hosting platform provider by virtue of operating the WordPress.com infrastructure.

We do not use Meta, TikTok, or LinkedIn advertising pixels, Google Analytics, or session-replay tools on the marketing website. We are evaluating whether any technologies used on the marketing website, including Jetpack Stats and the Blaze advertising module, constitute a ‘sale’ or ‘sharing’ of personal information under California law and will implement any required opt-out mechanism before this Privacy Policy takes effect.

Where required by applicable law, we honor browser-level and device-level opt-out preference signals.

12. DATA RETENTION

We retain personal information for no longer than reasonably necessary to fulfill the purposes for which it was collected, including to provide the Services, maintain your account, comply with legal and regulatory obligations, resolve disputes, and enforce our agreements. The table below sets out the specific retention periods that apply to each category of personal information we collect. Retention of Protected Health Information is governed by the HIPAA documents referenced in Section 2 and by applicable law. When personal information is no longer needed for any retained purpose, we delete or de-identify it.

Category of Personal Information	Retention Period
Account and identity information (name, email, username, credentials)	Duration of active account + 5 years after closure
Health and wellness data (wearable/HealthKit/EHR-derived data, provider-entered data, uploaded records, and raw imported device and clinical records)	7 years from date of collection or last service date
Usage and device information (interactions, device identifiers, logs, diagnostics)	2 years in identifiable form, then delete or de-identify
Location information (embedded in health file imports)	Tied to associated health record — 7 years
Communications and support records	5 years from date of communication
User content (uploads, submissions)	Duration of active account + 5 years after closure, unless earlier deletion is requested
Inferences	Deleted or de-identified when underlying account data is purged
Sensitive personal information	Same period as the applicable underlying category

13. DATA SECURITY

We maintain administrative, technical, and physical safeguards designed to protect personal information. No system is perfectly secure, and we cannot guarantee absolute security.

14. CHILDREN

The Services are not directed to children. You must be at least 18 years old to create an account or use the Services. We do not knowingly collect personal information from anyone under 18. Because the Services are restricted to users 18 and older, we do not knowingly collect personal information from children under 13 within the meaning of the Children's Online Privacy Protection Act (COPPA). If we learn that we have collected personal information from a person under 18, we will delete that information promptly. If you believe that a child has provided personal information to us through the Services, please contact us at privacy@bowerhouse.com.

15. INTERNATIONAL USERS

The Services are operated from the United States. If you access them from outside the United States, you understand that your information will be processed in the United States.

16. THIRD-PARTY SERVICES

The App integrates with third-party devices, platforms, and services that have their own privacy policies. We are not responsible for their practices. Review their policies before connecting them.

17. CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time. If we make material changes, we will provide notice through the Services or by other reasonable means before the changes take effect and, where required by applicable law, obtain your consent. Your continued use of the Services after the updated Privacy Policy takes effect constitutes your acknowledgment of the changes. The Effective Date above reflects the most recent revision.

18. CONTACT

Bower House Holdings, LLC

732 S 6th Street, #6952

Las Vegas, NV 89101

Privacy inquiries: privacy@bowerhouse.com

Privacy Choices: use the Privacy Choices setting in the App or on the Website, or contact privacy@bowerhouse.com