

bswing/AskBemsha Privacy Policy

Effective Date: January 1, 2026 | Last Reviewed: August 10, 2026

bswing and its sister company AskBemsha ("[Firm Name]," "we," "us," or "our") is a market research and consulting firm. This Privacy Policy explains how we collect, use, disclose, and protect personal information, including personal information relating to health, when we conduct research studies, focus groups, interviews, surveys, advisory boards, and related engagements ("Research Activities"), and when you visit our websites or interact with our recruitment and research platforms.

We are frequently engaged by pharmaceutical, medical device, payer, and healthcare clients ("Clients" or "Research Sponsors") to conduct research involving healthcare professionals ("HCPs"), patients, caregivers, and members of the general public. Because this work can involve sensitive health information, we design our privacy practices to meet or exceed the requirements of the EU/UK General Data Protection Regulation ("GDPR"), the U.S. Health Insurance Portability and Accountability Act ("HIPAA," where applicable), and applicable U.S. state privacy laws, and to align with the professional standards of the Insights Association, ESOMAR (ICC/ESOMAR International Code), and, where research involves interactions connected to pharmaceutical clients, the PhRMA Code on Interactions with Health Care Professionals.

1. Who We Are and How to Contact Us

bswing/AskBemsha acts as the data controller (or "business"/"processor," depending on the engagement) for personal information collected directly through our own recruitment channels, panels, and websites. When we conduct research on behalf of a Client, the Client is typically the data controller and AskBemsha acts as a data processor / service provider under a written data processing agreement. This Policy describes our practices in either role.

Privacy inquiries: privacy@bswing.com

Mailing address: 700 Washington Avenue North, Suite 204, Minneapolis, MN 55401

EU/UK Representative (if applicable): Not applicable at this time

2. Information We Collect

Depending on the Research Activity, we may collect the following categories of information:

2.1 Identifying and Contact Information

- Name, email address, phone number, mailing address
- Professional details for HCPs (specialty, license/NPI number, practice affiliation, years in practice)
- Demographic information (age, gender, income range, household composition)

2.2 Health and Medical Information (Special Category / Sensitive Data)

- Self-reported diagnosis, condition, symptoms, or treatment history relevant to the research topic
- Medication and treatment experience, including prescribing behavior (for HCP research)
- Caregiver relationship and care responsibilities
- Audio, video, or transcript content from interviews, focus groups, or diary studies that may reference health status

We collect health information only where it is necessary for the specific research objective, and only with your informed, explicit consent as described in Section 4.

2.3 Research Participation Data

- Survey responses, interview recordings and transcripts, discussion guide responses, diary/journal entries
- Screening questionnaire responses used to determine eligibility
- Incentive/honorarium payment information (name, address, tax ID where legally required)

2.4 Technical Information

- IP address, device/browser type, and platform usage data collected through our recruitment websites, survey tools, or video platforms
- Cookies and similar technologies, as described in our Cookie Notice

3. How We Use Information

We use personal information solely for the following purposes:

- Determining eligibility to participate in a research study
- Conducting and recording research sessions (surveys, interviews, focus groups, advisory boards, ethnographic or diary studies)
- Analyzing and reporting aggregated, de-identified, or pseudonymized insights to Research Sponsors
- Processing incentive/honorarium payments and complying with related tax reporting obligations
- Maintaining research integrity records (quality control, data validation, fraud/duplicate-participant detection)
- Complying with legal, regulatory, and professional-standards obligations (including PhRMA Code transparency and reporting requirements, where applicable)

We do not use personal information collected for a specific study for unrelated marketing purposes, and we do not sell personal information, consistent with the Insights Association Code of Standards and Ethics and the ICC/ESOMAR International Code.

4. Our Legal Bases for Processing (GDPR)

Where GDPR applies, we rely on the following legal bases:

- Explicit consent (Art. 9(2)(a)) — for special category data, including health information; consent is obtained separately from general study consent and can be withdrawn at any time
- Consent (Art. 6(1)(a)) — for general participation, recording, and use of contact details
- Legitimate interests (Art. 6(1)(f)) — for research quality/fraud prevention and business administration, balanced against your rights and never used to justify processing of health data without consent
- Legal obligation (Art. 6(1)(c)) — for tax reporting on incentive payments and regulatory recordkeeping

Where research falls outside GDPR (e.g., U.S. participants), we apply the same consent-first standard as a matter of firm policy, not merely legal minimum compliance.

5. HIPAA and Protected Health Information

bswing/AskBemsha is generally not a "Covered Entity" under HIPAA. In most market research engagements, participants (or their caregivers) self-report health information directly to us; this self-reported information is not "Protected Health Information" (PHI) governed by HIPAA because it does not originate from a Covered Entity's medical records.

In engagements where Bswing/AskBemsha receives information originating from a Covered Entity (for example, a health plan, hospital system, or medical record source) on behalf of a Client, we require a Business Associate Agreement ("BAA") before receiving that data, and we handle it in accordance with the HIPAA Privacy, Security, and Breach Notification Rules, including:

- Minimum necessary use and disclosure
- De-identification using the HIPAA Safe Harbor method (removal of the 18 identifiers) or Expert Determination, prior to sharing insights externally where feasible
- Administrative, physical, and technical safeguards consistent with the HIPAA Security Rule
- Breach notification to the applicable Covered Entity/Client within contractually required timeframes

For HCP research where PHI-adjacent clinical scenarios or case studies are discussed, we require that any patient details shared verbally be de-identified or fictionalized by the HCP participant, and we instruct moderators accordingly.

6. How We Share Information

We disclose personal information only as follows:

- To Research Sponsors: In aggregated or de-identified form (e.g., "6 of 12 respondents indicated..."). Verbatim quotes or identifiable video/audio clips are shared only with your specific additional consent.
- To subcontractors and processors who support our operations (e.g., recruitment panels, transcription vendors, translation services, secure video platforms, payment processors), each bound by written data processing / confidentiality agreements requiring protections equivalent to this Policy.
- To professional advisors, auditors, or regulators as required by law, or to support our SOC 2 Type 2 audit process.
- In connection with a corporate transaction (merger, acquisition, financing), subject to confidentiality commitments.

We do not sell, rent, or trade personal information to third parties for their own marketing purposes.

7. Data Retention

We retain personal information only as long as necessary for the purposes described in this Policy, generally:

- Raw recordings and transcripts: Retained per the Client contract, typically 24 months post-project, then securely deleted or fully anonymized
- Screening/eligibility data for non-selected candidates: Deleted within 12 months absent re-contact permission
- Incentive payment records: Retained as required by tax law (typically 7 years in the U.S.)
- Aggregated, de-identified insights: May be retained indefinitely, as they no longer constitute personal information

8. Data Security

Bswing/AskBemsha maintains a security program aligned with the AICPA SOC 2 Type 2 Trust Services Criteria (security, availability, confidentiality, and, where applicable, processing integrity and privacy). Our controls include, at minimum:

- Encryption of personal data in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access controls and least-privilege permissions, with periodic access reviews
- Multi-factor authentication for systems housing research participant data

- Continuous logging and monitoring, with retained audit trails
- Annual (or more frequent) third-party penetration testing and an independent SOC 2 Type 2 audit
- Formal vendor risk management, including due diligence and contractual security requirements for subcontractors
- Documented incident response and breach notification procedures

Our current SOC 2 Type 2 report [in progress, anticipate final approval Q1 2027] is available to Clients and prospective Clients under NDA upon request.

9. International Data Transfers

Where personal information is transferred outside the European Economic Area, United Kingdom, or Switzerland, we rely on appropriate safeguards, including the European Commission's Standard Contractual Clauses (SCCs), the UK International Data Transfer Addendum, and, where applicable, participation in recognized transfer frameworks. We conduct transfer impact assessments for high-risk transfers involving sensitive health data.

10. Your Privacy Rights

10.1 Rights for EEA/UK/Swiss Residents (GDPR)

- Right to access a copy of your personal information
- Right to rectification of inaccurate information
- Right to erasure ("right to be forgotten"), subject to legal retention obligations
- Right to restrict or object to processing
- Right to data portability
- Right to withdraw consent at any time, without affecting prior lawful processing
- Right to lodge a complaint with your local Data Protection Authority

10.2 Rights for U.S. Residents

Depending on your state of residence (e.g., California, Colorado, Connecticut, Virginia, and other states with comprehensive privacy laws), you may have rights to know, delete, correct, or opt out of certain processing of your personal information, and the right to non-discrimination for exercising these rights.

To exercise any of these rights, contact us at the email address in Section 1. We will respond within the timeframe required by applicable law (generally 30 days, extendable where permitted).

11. Children's Privacy

Our Research Activities are directed to adults. We do not knowingly collect personal information from individuals under 18 without verified parental/guardian consent and, where relevant, additional safeguards required for research involving minors (e.g., pediatric caregiver studies). We will provide an overview of our children's privacy policies and standard operating procedures, please email privacy@bswing.com to request it.

12. Cookies and Website Tracking

Our recruitment and survey websites may use cookies and similar technologies to operate securely, prevent duplicate participation, and understand aggregate site usage. Where required by law, we present a cookie consent banner allowing you to accept or decline non-essential cookies. See our separate Cookie Notice for details.

13. Professional Standards

bswing/AskBemsha designs its research practices to comply with the Insights Association Code of Standards and Ethics for Market Research, the ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics, and — for engagements connected to pharmaceutical Clients — the PhRMA Code on Interactions with Health Care Professionals. Consistent with these codes, we:

- Never use research contact as a guise for sales or promotional activity
- Always identify ourselves and the general nature of the research (subject to legitimate blinding of the Client's identity)
- Honor all requests to withdraw from a study at any time without penalty
- Ensure incentives are reasonable and not coercive, and are reported in compliance with applicable transparency requirements

14. Changes to This Policy

We may update this Policy from time to time. The "Last Reviewed" date above reflects the most recent revision. Material changes will be posted on our website, and, where required by law, we will provide additional notice.

15. Contact Us

Questions, requests, or complaints regarding this Policy or our data practices can be directed to:

Privacy Officer / Data Protection Officer

privacy@bswing.com

bswing, inc.
5100 West 36th Street, #16167
Minneapolis, MN 55416