

PRIVACY POLICY

SACCADE, INC.

a Delaware corporation

Principal place of business: San Francisco, California

Version 1.0

Adopted June 1, 2026

Effective June 1, 2026

Reviewed and reaffirmed without amendment September 19, 2026

Governing the website at saccade.com, the Patient Interest Program, the Clinic Partner Program, and related communications, and constituting the Company's Consumer Health Data Privacy Policy under Wash. Rev. Code Chapter 19.373 and its Notice at Collection under Cal. Civ. Code Section 1798.100.

Privacy Officer: privacy@saccade.com

Security: security@saccade.com

Rights requests: saccade.com/privacy-request

TABLE OF CONTENTS

ARTICLE 1. PRELIMINARY PROVISIONS
ARTICLE 2. DEFINITIONS
ARTICLE 3. THE COMPANY'S ROLES AND REGULATORY STATUS
ARTICLE 4. CATEGORIES OF PERSONAL INFORMATION COLLECTED, SOURCES, AND PURPOSES
ARTICLE 5. THE PATIENT INTEREST PROGRAM
ARTICLE 6. THE CLINIC PARTNER PROGRAM
ARTICLE 7. CLINICAL DATA AND PARTNER CLINIC OPERATIONS
ARTICLE 8. PURPOSES OF PROCESSING AND LEGAL BASES
ARTICLE 9. DISCLOSURE OF PERSONAL INFORMATION
ARTICLE 10. COOKIES, ANALYTICS, SESSION REPLAY, AND TRACKING SIGNALS
ARTICLE 11. COMMUNICATIONS, MARKETING, AND TELEPHONE CONSENT
ARTICLE 12. SECURITY
ARTICLE 13. DATA RETENTION
ARTICLE 14. RIGHTS OF INDIVIDUALS AND HOW TO EXERCISE THEM
ARTICLE 15. CHILDREN AND MINORS
ARTICLE 16. INTERNATIONAL VISITORS AND CROSS-BORDER TRANSFERS
ARTICLE 17. THIRD-PARTY SITES AND SERVICES
ARTICLE 18. AUTOMATED DECISION-MAKING AND PROFILING
ARTICLE 19. AMENDMENT OF THIS POLICY
ARTICLE 20. GENERAL PROVISIONS
ARTICLE 21. CONTACT INFORMATION
APPENDIX A. CONSENT LANGUAGE AND FORM SPECIFICATIONS
APPENDIX B. CALIFORNIA DISCLOSURES: CATEGORIES OF PERSONAL INFORMATION
APPENDIX C. PROCESSORS
APPENDIX D. RETENTION SCHEDULE
APPENDIX E. CALIFORNIA NOTICE AT COLLECTION
APPENDIX F. VERSION HISTORY
CERTIFICATE OF ADOPTION

ARTICLE 1. PRELIMINARY PROVISIONS

1.1 Adoption and Effective Date. This Privacy Policy (this "Policy") was adopted by Saccade, Inc., a Delaware corporation having its principal place of business in San Francisco, California (the "Company," "Saccade," "we," "us," or "our"), on June 1, 2026, and is effective as of June 1, 2026 (the "Effective Date"). This Policy is designated Version 1.0. No prior version of this Policy exists. This Policy was reviewed and reaffirmed without amendment on September 19, 2026.

1.2 Scope. This Policy governs the collection, use, storage, disclosure, transfer, retention, and other Processing of Personal Information and Consumer Health Data by the Company in connection with (a) the website located at saccade.com and every subdomain, page, and form thereof (collectively, the "Site"); (b) the Patient Interest Program described in Article 5; (c) the Clinic Partner Program described in Article 6; (d) electronic mail, telephone, short message service ("SMS"), and other communications between the Company and any Individual; and (e) any other online or offline interaction that references or links to this Policy (items (a) through (e), collectively, the "Services").

1.3 Exclusions from Scope. This Policy does not govern (a) Clinical Data, as defined in Article 2, which is governed exclusively by Article 7, by the privacy notice of the Partner Clinic that generated it, and by the written agreements between the Company and that Partner Clinic; (b) Personal Information Processed by the Company in its capacity as an employer or prospective employer, which is governed by a separate workforce privacy notice; (c) Personal Information of the Company's investors, lenders, and professional advisors, which is governed by the agreements with those parties; or (d) any third-party website, application, or service, including any Partner Clinic website, regardless of whether the Site links to it.

1.4 Acceptance. By accessing or using the Site or the Services, by submitting any form on the Site, or by otherwise providing Personal Information to the Company, an Individual acknowledges that he or she has read and understood this Policy. Where applicable law requires consent as the basis for a particular Processing activity, the Company obtains that consent separately and affirmatively as described in Article 8 and Appendix A, and mere use of the Site does not constitute such consent.

1.5 Relationship to Other Terms. This Policy is incorporated by reference into the Company's Terms of Use for the Site. In the event of a direct conflict between this Policy and the Terms of Use concerning the Processing of Personal Information, this Policy controls. In the event of a direct conflict between this Policy and a written Business Associate Agreement, Data Processing Agreement, or Partner Clinic Agreement executed by the Company, the executed agreement controls with respect to the data and parties it covers.

1.6 Interpretation. Article and section headings are for convenience only and do not affect interpretation. The words "include," "includes," and "including" are deemed to be followed by "without limitation." The singular includes the plural and vice versa. References to a statute or regulation include that statute or regulation as amended, re-enacted, or replaced from time to time, and any regulations promulgated thereunder. Where this Policy states that the Company "does not" engage in a practice, that statement is a present commitment that the Company will not engage in that practice for so long as this Policy remains in effect without amendment under Article 19.

ARTICLE 2. DEFINITIONS

2.1 "Aggregated Data" means information that relates to a group or category of Individuals, from which individual identities have been removed, and that is not linked or reasonably linkable to any Individual or household.

2.2 "Applicant" means any Individual who submits, or begins to submit, a Clinic Partner Application on behalf of a Clinic.

2.3 "Business Associate Agreement" or "BAA" means a written agreement that satisfies the requirements of 45 C.F.R. Sections 164.502(e) and 164.504(e) under the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations (collectively, "HIPAA").

2.4 "Clinic" means a medical practice, longevity or preventive-health practice, neurology practice, primary-care practice, concierge medical practice, health system, or other licensed healthcare provider organization.

2.5 "Clinic Partner Application" means the form on the Site through which an Applicant applies for a Clinic to become a Partner Clinic, and any information submitted through it.

2.6 "Clinical Data" means any information, in any form, generated by, derived from, or relating to the administration of the Saccade Assessment to an Individual at a Partner Clinic, including eye-tracking recordings, ocular images, derived metrics, calibration data, assessment results, reports, and any Protected Health Information within the meaning of 45 C.F.R. Section 160.103.

2.7 "Consumer Health Data" means Personal Information that is linked or reasonably linkable to an Individual and that identifies the Individual's past, present, or future physical or mental health status, as that term or its equivalent is defined in the Washington My Health My Data Act, Wash. Rev. Code Chapter 19.373; Nevada Senate Bill 370 (2023), Nev. Rev. Stat. Chapter 603A as amended; the Connecticut Data Privacy Act, Conn. Gen. Stat. Section 42-515 et seq.; and any other applicable law of similar effect. For the avoidance of doubt, and without limiting the foregoing definitions, the Company treats the following as Consumer Health Data: (a) the fact that an Individual has submitted a Patient Interest Submission; (b) an Individual's response to the Optional Health Question; and (c) any inference the Company draws from (a) or (b) concerning an Individual's health.

2.8 "Controller" means the natural or legal person that, alone or jointly with others, determines the purposes and means of Processing Personal Information, and includes a "business" as defined in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"), Cal. Civ. Code Section 1798.100 et seq.

2.9 "De-identified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable Individual, provided that the Company (a) takes reasonable measures to ensure that the data cannot be associated with an Individual; (b) publicly commits to Process the data only in de-identified form and not to attempt to re-identify it; and (c) contractually obligates any recipient of the data to comply with the same requirements.

2.10 "Individual," "you," and "your" mean any natural person whose Personal Information is Processed under this Policy, including Visitors, Registrants, and Applicants.

2.11 "Optional Health Question" means the single question on the Patient Interest Form that asks whether the Individual, or the person on whose behalf the Individual is inquiring, has noticed any changes in memory or thinking, together with the response options set forth in Appendix A.

2.12 "Partner Clinic" means a Clinic that has executed a Partner Clinic Agreement and a Business Associate Agreement with the Company and is authorized to administer the Saccade Assessment.

2.13 "Patient Interest Form" means the form on the Site, currently located at saccade.com/get-tested, through which an Individual asks to be matched with a Partner Clinic.

2.14 "Patient Interest Submission" means a completed or partially completed Patient Interest Form and all information contained in it.

2.15 "Personal Information" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Individual or household. Personal Information includes "personal data" as defined in applicable state privacy laws and "personal data" as defined in Article 4(1) of Regulation (EU) 2016/679 (the "GDPR"). Personal Information does not include Aggregated Data, De-identified Data, or publicly available information as defined by applicable law.

2.16 "Processing" or "Process" means any operation or set of operations performed on Personal Information, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

2.17 "Processor" or "Service Provider" means a natural or legal person that Processes Personal Information on behalf of, and under the documented instructions of, the Company, and includes a "service provider" and "contractor" as defined in the CCPA and a "processor" as defined in other applicable state privacy laws and the GDPR.

2.18 "Registrant" means any Individual who submits, or begins to submit, a Patient Interest Form.

2.19 "Saccade Assessment" means the Company's eye-movement assessment administered by means of a head-mounted display and associated software and hardware, in whatever version exists from time to time.

2.20 "Sale," "Sell," or "Sold" means the exchange of Personal Information for monetary or other valuable consideration, as defined in the CCPA and other applicable state privacy laws, and, with respect to Consumer Health Data, as defined in Wash. Rev. Code Section 19.373.010.

2.21 "Sensitive Personal Information" means Personal Information that reveals an Individual's racial or ethnic origin, religious or philosophical beliefs, citizenship or immigration status, mental or physical health diagnosis or condition, sex life or sexual orientation, genetic data, biometric data Processed for the purpose of uniquely identifying an Individual, precise geolocation, government-issued identification numbers, account log-in credentials, financial account information, or the contents of an Individual's mail, email, or text messages where the Company is not the intended recipient, and includes "sensitive personal information" and "sensitive data" as defined in applicable state privacy laws and "special categories of personal data" as defined in Article 9 of the GDPR.

2.22 "Share" or "Sharing" means the disclosure of Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, as defined in Cal. Civ. Code Section 1798.140(ah).

2.23 "Targeted Advertising" means displaying an advertisement to an Individual where the advertisement is selected based on Personal Information obtained from that Individual's activities over time and across nonaffiliated websites or online applications, as defined in applicable state privacy laws.

2.24 "Visitor" means any Individual who accesses the Site, whether or not the Individual submits any form.

ARTICLE 3. THE COMPANY'S ROLES AND REGULATORY STATUS

3.1 Controller of Site Data. With respect to all Personal Information collected through the Site and the Services, the Company acts as a Controller and is responsible for the Processing described in this Policy.

3.2 Business Associate with Respect to Clinical Data. With respect to Clinical Data, the Company acts as a Business Associate, within the meaning of 45 C.F.R. Section 160.103, of the Partner Clinic that administers the Saccade Assessment. The Company Processes Clinical Data solely as permitted by the applicable Business Associate Agreement, the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E), the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C), and the HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D). Article 7 describes this relationship further.

3.3 The Company Is Not a Covered Entity with Respect to the Site. The Company is not a health care provider, health plan, or health care clearinghouse within the meaning of 45 C.F.R. Section 160.103, does not bill for or furnish health care through the Site, and does not transmit health information in connection with any transaction for which the Secretary of Health and Human Services has adopted a standard. Accordingly, Personal Information submitted through the Site, including a response to the Optional Health Question, is not Protected Health Information under HIPAA when it is submitted, and the Company's obligations with respect to such information arise under the Federal Trade Commission Act, 15 U.S.C. Section 45; the FTC Health Breach Notification Rule, 16 C.F.R. Part 318, to the extent applicable; the state laws identified in Article 14; and this Policy. The Company nonetheless applies the safeguards described in Article 12 to all Consumer Health Data whether or not any law requires it.

3.4 No Patient Relationship. Submitting a Patient Interest Form, receiving communications from the Company, or being matched with a Partner Clinic does not create a physician-patient, provider-patient, or any other clinical relationship between the Individual and the Company. Any clinical relationship exists solely between the Individual and the Partner Clinic.

3.5 Not Medical Advice; No Diagnosis. Nothing on the Site, in this Policy, in any communication from the Company, or in any matching decision constitutes medical advice, a diagnosis, a screening result, a risk score, a prognosis, or a recommendation for or against any treatment. The Saccade Assessment is administered and interpreted only by Partner Clinics. The Company does not communicate assessment results to Individuals through the Site or through the communications channels described in this Policy. An Individual who is experiencing a medical emergency should contact emergency services immediately.

3.6 Regulatory Status of the Saccade Assessment. The Saccade Assessment is under development. Its regulatory status, intended use, and any clearance, approval, authorization, or exemption obtained from the United States Food and Drug Administration or any other regulator are stated on the Site's "About" page as updated from time to time, and nothing in this Policy shall be construed as a representation concerning that status.

ARTICLE 4. CATEGORIES OF PERSONAL INFORMATION COLLECTED, SOURCES, AND PURPOSES

4.1 Information Individuals Provide Directly.

(a) Patient Interest Submissions. When an Individual submits a Patient Interest Form, the Company collects: (i) first name; (ii) email address; (iii) telephone number, if the Individual chooses to provide it; (iv) five-digit United States postal ZIP code; (v) age in years; (vi) the Individual's selection

indicating whether the assessment is sought for the Individual, a parent, a spouse or partner, or another person; (vii) the Individual's selection, if any, indicating how the Individual learned of the Company; (viii) the Individual's response, if any, to the Optional Health Question; (ix) the Individual's consent selections and the date, time, and Internet Protocol address at which each consent was given; and (x) the Site page and referring source from which the form was submitted.

(b) Clinic Partner Applications. When an Applicant submits a Clinic Partner Application, the Company collects: (i) the Applicant's name; (ii) the Applicant's role at the Clinic; (iii) the Applicant's work email address; (iv) the Applicant's telephone number, if provided; (v) the Clinic's name; (vi) the Clinic's website address, if provided; (vii) the Clinic's city and state; (viii) the Clinic's practice type; (ix) the Clinic's approximate monthly patient volume, expressed as a range; (x) the categories of cognitive or biomarker screening the Clinic currently offers; (xi) the number of Clinic locations, expressed as a range, if provided; (xii) any free-text statement the Applicant chooses to provide; (xiii) the Applicant's consent selection and the date, time, and Internet Protocol address at which it was given; and (xiv) the Site page and referring source from which the form was submitted.

(c) Communications. When an Individual communicates with the Company by email, telephone, SMS, web form, or postal mail, the Company collects the content of the communication, the Individual's contact details, and the date and time of the communication. Telephone calls are not recorded. SMS messages are retained as described in Article 11.

(d) Surveys and Feedback. If the Company invites an Individual to complete a survey or provide feedback and the Individual chooses to do so, the Company collects the responses provided. Participation is voluntary, and each survey states its purpose at the point of collection.

4.2 Information Collected Automatically. When an Individual accesses the Site, the Company and the Processor identified in Article 9.3 automatically collect: (a) Internet Protocol address, from which an approximate geographic location at the city or region level is derived and after which the full address is truncated or discarded as described in Article 10.4; (b) browser type and version; (c) operating system and device type; (d) screen resolution and viewport dimensions; (e) preferred language; (f) the address of the web page that referred the Individual to the Site and any campaign parameters contained in the Site's address; (g) the pages viewed, the order in which they were viewed, and the time spent on each; (h) clicks, scrolling, cursor movement, form-field focus and blur events, and other interaction events, excluding the content of any form field, which is masked at the point of collection as described in Article 10.3; (i) the date and time of each request; and (j) cookie identifiers and similar identifiers described in Article 10. This information is collected through cookies, pixels, scripts, and server logs.

4.3 Information Collected from Third Parties. The Company collects Personal Information from the following third-party sources only: (a) from a Partner Clinic, confirmation that a matched Registrant has or has not scheduled or attended an appointment, limited to the Registrant's name, the date of the confirmation, and a status indicator, and excluding any Clinical Data; (b) from publicly available professional and business registries, including the National Plan and Provider Enumeration System and state medical board licensing databases, information used to verify that a Clinic named in a Clinic Partner Application exists and is licensed; (c) from the Clinic's own public website, information used for the same verification purpose; and (d) from the Company's email Processor, delivery, bounce, open, and click metadata concerning messages the Company sends. The Company does not purchase Personal Information from data brokers and does not append demographic, financial, or health data from any third-party source.

4.4 Inferences. The Company draws the following inferences, and no others, from the Personal Information described in this Article: (a) the geographic region in which a Registrant is likely seeking an assessment, derived from the ZIP code; (b) the Registrant's likely priority for matching, derived from age, the person on whose behalf the inquiry is made, and, if answered, the response to the Optional Health Question; and (c) the likely size and fit of a Clinic, derived from the Clinic Partner Application. The Company does not draw inferences for the purpose of advertising, and does not create or maintain a profile of any Individual for use in Targeted Advertising.

4.5 Purposes of Collection. The Company collects the Personal Information described in this Article for the purposes enumerated in Article 8 and for no other purpose. The Company collects only the Personal Information that is adequate, relevant, and reasonably necessary for those purposes.

4.6 Consequences of Not Providing Information. Fields on the Patient Interest Form and the Clinic Partner Application that are marked as required are necessary for the Company to perform the matching or application-review function requested. An Individual who declines to provide required information may not submit the form. Fields marked as optional, including the telephone number, the referral source, the Clinic website, the number of locations, the free-text statement, and the Optional Health Question, may be left blank without any effect on the Individual's ability to submit the form or on the Company's willingness to consider the submission.

ARTICLE 5. THE PATIENT INTEREST PROGRAM

5.1 Description. The Patient Interest Program allows an Individual to indicate interest in undergoing the Saccade Assessment and to ask the Company to notify the Individual when a Partner Clinic is available within a reasonable distance of the Individual's ZIP code and, upon the Individual's confirmation, to introduce the Individual to that Partner Clinic.

5.2 Matching Process. When a Partner Clinic becomes available in a region, the Company identifies Registrants whose ZIP codes fall within the Partner Clinic's service area and contacts each such Registrant by email, and by telephone or SMS only if the Registrant has provided a telephone number and consented under Article 11, to inform the Registrant that a Partner Clinic is available. The Company discloses a Registrant's Personal Information to a Partner Clinic only after the Registrant has affirmatively confirmed, in response to that communication, that he or she wishes to be introduced to that specific Partner Clinic. The Company does not disclose any Registrant's Personal Information to any Clinic before such confirmation, and does not disclose it to more than one Partner Clinic without a separate confirmation for each.

5.3 Information Disclosed to a Partner Clinic upon Confirmation. Upon a Registrant's confirmation under Section 5.2, the Company discloses to the confirmed Partner Clinic only: (a) the Registrant's first name; (b) email address; (c) telephone number, if provided; (d) ZIP code; (e) age; (f) whether the assessment is sought for the Registrant or another person; and (g) the Registrant's response to the Optional Health Question, if and only if the Registrant gave the Health Data Consent described in Article 8.4 and Appendix A. The Company does not disclose the referral source, consent metadata, Internet Protocol address, or any automatically collected information described in Article 4.2 to any Partner Clinic.

5.4 Independent Responsibility of Partner Clinics. Upon receipt of a Registrant's Personal Information under Section 5.3, the Partner Clinic becomes an independent Controller of that information and is responsible for its subsequent Processing under the Partner Clinic's own privacy notice and applicable law. The Company contractually requires each Partner Clinic to (a) use the information solely to contact the

Registrant about scheduling the Saccade Assessment; (b) refrain from Selling or Sharing it; (c) refrain from using it for Targeted Advertising; (d) delete it upon the Registrant's request; and (e) maintain reasonable security measures. The Company is not responsible for a Partner Clinic's breach of those obligations but will, upon notice, take the remedial steps described in Article 9.7.

5.5 Prioritization. Where more Registrants exist in a Partner Clinic's service area than the Partner Clinic can accommodate in a given period, the Company may prioritize outreach based on the order in which Patient Interest Submissions were received, the age of the person for whom the assessment is sought, and, if answered, the response to the Optional Health Question. This prioritization affects only the order in which the Company sends the communication described in Section 5.2. It does not deny any Registrant access to any Partner Clinic, does not produce legal or similarly significant effects concerning any Individual, and is reviewed by a member of the Company's staff before any communication is sent.

5.6 Withdrawal. A Registrant may withdraw from the Patient Interest Program at any time by the means described in Article 14.9. Upon withdrawal, the Company ceases all outreach, deletes the Registrant's Patient Interest Submission in accordance with Article 13, and, if the Registrant's information has been disclosed to a Partner Clinic, notifies that Partner Clinic of the withdrawal and instructs it to delete the information.

ARTICLE 6. THE CLINIC PARTNER PROGRAM

6.1 Description. The Clinic Partner Program allows a Clinic to apply to become a Partner Clinic. The Company reviews each Clinic Partner Application, may contact the Applicant to obtain additional information or to schedule a demonstration, and may offer the Clinic a Partner Clinic Agreement.

6.2 Business Contact Information. The Personal Information collected through a Clinic Partner Application is collected in the Applicant's capacity as a representative of a Clinic and is used for business-to-business purposes. Where applicable law exempts such information from certain obligations, the Company relies on that exemption only to the extent the law provides, and otherwise treats the information as Personal Information under this Policy.

6.3 Verification. The Company may verify the information in a Clinic Partner Application using the public sources described in Article 4.3(b) and (c). The Company does not obtain consumer reports, credit reports, or background checks on any Applicant in connection with the Clinic Partner Program.

6.4 Use of Application Information. The Company uses Clinic Partner Application information to (a) evaluate the Clinic's suitability for the program; (b) communicate with the Applicant about the application, demonstrations, onboarding, and contracting; (c) plan the geographic expansion of the program; and (d) maintain records of applications received. The Company does not use Applicant information for Targeted Advertising and does not disclose it to any other Clinic.

6.5 Unsuccessful Applications. If the Company declines an application or the Clinic does not execute a Partner Clinic Agreement, the Company retains the application for the period stated in Article 13 and then deletes it, unless the Applicant requests earlier deletion under Article 14.

ARTICLE 7. CLINICAL DATA AND PARTNER CLINIC OPERATIONS

7.1 Governing Framework. Clinical Data is Processed by the Company solely as a Business Associate of the Partner Clinic that administered the Saccade Assessment, under a Business Associate Agreement executed before any Clinical Data is created, and in compliance with HIPAA. This Policy does not describe, and the Site is not used for, the collection, storage, or transmission of Clinical Data.

7.2 Notice of Privacy Practices. Each Partner Clinic provides its patients with a Notice of Privacy Practices as required by 45 C.F.R. Section 164.520. An Individual's rights with respect to Clinical Data, including rights of access, amendment, accounting of disclosures, and restriction, are exercised through the Partner Clinic in accordance with that notice and 45 C.F.R. Sections 164.522 through 164.528.

7.3 Segregation. The Company maintains Clinical Data in systems that are logically and administratively separate from the systems that hold Personal Information collected through the Site. The Company does not combine, link, or cross-reference Clinical Data with Patient Interest Submissions, Clinic Partner Applications, or automatically collected Site data, except that the Company may record, in the Patient Interest Program records, the fact that a Registrant attended an appointment, as described in Article 4.3(a), without any Clinical Data.

7.4 Biometric Information. The Saccade Assessment records eye movements and may capture images of the eye. Such recordings and images are Clinical Data governed by Article 7.1 and by the Partner Clinic's own compliance with any applicable biometric privacy law, including the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq., the Texas Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code Section 503.001, and Wash. Rev. Code Section 19.375. The Site does not collect biometric identifiers or biometric information from any Visitor, Registrant, or Applicant.

7.5 Research Use. The Company does not use Clinical Data for research except as expressly permitted by the applicable Business Associate Agreement and, where required, by an Institutional Review Board-approved protocol and the informed consent or authorization of the Individual under 45 C.F.R. Section 164.508 or a waiver under 45 C.F.R. Section 164.512(i). Any such research is described in documents provided to the Individual by the Partner Clinic or the research site, not in this Policy.

ARTICLE 8. PURPOSES OF PROCESSING AND LEGAL BASES

8.1 Enumerated Purposes. The Company Processes Personal Information for the following purposes only:

- (a) to operate the Patient Interest Program, including to receive and store Patient Interest Submissions, to determine which Partner Clinics serve a Registrant's region, to communicate the availability of a Partner Clinic, and, upon confirmation, to introduce the Registrant to that Partner Clinic;
- (b) to operate the Clinic Partner Program, including to receive, verify, and evaluate Clinic Partner Applications and to communicate with Applicants;
- (c) to respond to inquiries, requests, and complaints and to provide support;
- (d) to send transactional and service communications, including confirmations of form submissions, responses to requests under Article 14, and notices required by law or by this Policy;
- (e) to send informational communications about the Company and the availability of the Saccade Assessment to Individuals who have consented to receive them, subject to the opt-out rights described

in Article 11;

(f) to measure, analyze, and improve the performance, usability, and content of the Site, using the automatically collected information described in Article 4.2;

(g) to detect, investigate, and prevent fraudulent submissions, abuse, security incidents, and other harmful or unlawful activity, and to protect the rights, property, and safety of the Company, Individuals, Partner Clinics, and the public;

(h) to comply with applicable law, regulation, legal process, and governmental request, and to establish, exercise, or defend legal claims;

(i) to maintain records of consents given and withdrawn, requests received and fulfilled, and other matters that applicable law requires the Company to document;

(j) to plan the geographic expansion of the Patient Interest Program and the Clinic Partner Program, using Aggregated Data and De-identified Data wherever possible; and

(k) to effect a corporate transaction described in Article 9.6.

8.2 Prohibited Purposes. The Company does not, and commits that it will not, Process Personal Information collected under this Policy for any of the following purposes: (a) Selling Personal Information or Consumer Health Data; (b) Sharing Personal Information for cross-context behavioral advertising; (c) Targeted Advertising; (d) profiling in furtherance of decisions that produce legal or similarly significant effects concerning an Individual; (e) determining eligibility for, or the price of, insurance, credit, employment, housing, or any other benefit; (f) disclosure to any employer, insurer, or governmental agency except as compelled by law under Article 9.5; or (g) any purpose incompatible with the purposes for which the information was collected, unless the Company first obtains the Individual's consent to the new purpose.

8.3 Legal Bases (Where Required). Where applicable law, including the GDPR, requires a legal basis for Processing, the Company relies on the following: (a) performance of a contract or steps taken at the Individual's request before entering into a contract, GDPR Article 6(1)(b), for the purposes in Sections 8.1(a) through (d); (b) the Company's legitimate interests, GDPR Article 6(1)(f), for the purposes in Sections 8.1(f), (g), (j), and (k), which interests are operating and securing the Site and planning the Company's business, and which the Company has determined are not overridden by the interests or fundamental rights of Individuals given the limited data involved and the safeguards described in this Policy; (c) compliance with a legal obligation, GDPR Article 6(1)(c), for the purposes in Sections 8.1(h) and (i); and (d) consent, GDPR Article 6(1)(a), for the purpose in Section 8.1(e) and for the placement of non-essential cookies under Article 10.

8.4 Explicit Consent for Consumer Health Data. The Company Processes an Individual's response to the Optional Health Question, and discloses it to a Partner Clinic, only on the basis of the Individual's explicit, affirmative, opt-in consent (the "Health Data Consent"), obtained by means of a checkbox that is unchecked by default, is presented separately from every other consent and from the Terms of Use, is accompanied by the text set forth in Appendix A, and is displayed only when the Individual has entered a response to the Optional Health Question. The Health Data Consent constitutes (a) "consent" within the meaning of Wash. Rev. Code Section 19.373.010(6) and (b) explicit consent within the meaning of GDPR Article 9(2)(a), where applicable. If the Health Data Consent is not given, the Company does not store the response to the Optional Health Question, and the form may be submitted without it.

8.5 Consent for Contact. The Company contacts a Registrant about the Patient Interest Program, and an Applicant about the Clinic Partner Program, on the basis of the affirmative consent obtained by means of the checkboxes described in Appendix A (the "Contact Consent"), which are unchecked by default and are required to submit the respective forms.

8.6 Withdrawal of Consent. An Individual may withdraw any consent at any time by the means described in Article 14.9. Withdrawal takes effect prospectively and does not affect the lawfulness of Processing carried out before withdrawal. Upon withdrawal of the Health Data Consent, the Company deletes the response to the Optional Health Question within the period stated in Article 14.10 and instructs any Partner Clinic that received it to do the same. Upon withdrawal of the Contact Consent, the Company treats the Registrant or Applicant as having withdrawn from the applicable program under Section 5.6 or Section 6.5.

ARTICLE 9. DISCLOSURE OF PERSONAL INFORMATION

9.1 General Rule. The Company discloses Personal Information only to the categories of recipients described in this Article, only for the purposes described in Article 8, and only to the extent reasonably necessary for those purposes. The Company has not Sold or Shared Personal Information, and has not Sold Consumer Health Data, at any time in the twelve months preceding the Effective Date, and does not do so.

9.2 Partner Clinics. The Company discloses the Personal Information described in Section 5.3 to a single confirmed Partner Clinic, subject to the conditions in Article 5. The Company discloses Applicant information to no Clinic other than the Applicant's own.

9.3 Processors. The Company engages the following categories of Processors, each of which Processes Personal Information solely on the Company's documented instructions, under a written contract that satisfies Cal. Civ. Code Section 1798.100(d), Cal. Code Regs. tit. 11, Section 7051, and the equivalent provisions of other applicable state privacy laws and GDPR Article 28, and that prohibits the Processor from Selling, Sharing, retaining, using, or disclosing the Personal Information for any purpose other than performing the contracted services:

- (a) database hosting and storage: Supabase, Inc., which hosts the databases in which Patient Interest Submissions and Clinic Partner Applications are stored, on infrastructure located in the United States;
- (b) website hosting and content delivery: Vercel Inc., which hosts the Site and processes server requests, including Internet Protocol addresses, in the course of serving pages;
- (c) product analytics and session replay: PostHog, Inc., which collects and processes the automatically collected information described in Article 4.2 on the Company's behalf, on infrastructure located in the United States, with form-field content masked and Internet Protocol addresses processed as described in Article 10;
- (d) transactional email delivery: Resend, Inc., which transmits the email communications described in Section 8.1(d) and (e) and returns delivery metadata to the Company;
- (e) internal notifications: Slack Technologies, LLC, a Salesforce company, which receives, upon each form submission, a notification containing only the form type, the city and state derived from the ZIP code or entered by the Applicant, the timestamp, and a link to the record in the Company's database, and which does not receive any name, email address, telephone number, age, or response to the Optional Health Question;

(f) business productivity and email: Google LLC, through Google Workspace, which hosts the Company's business email accounts and documents and through which staff communicate with Individuals; and

(g) telephone and SMS communications, if and when the Company sends SMS messages under Article 11: a telecommunications Processor engaged under a written contract meeting the requirements of this Section, the identity of which the Company will add to Appendix C before sending any SMS message.

A current list of Processors, with their locations and functions, is maintained in Appendix C and is updated in accordance with Article 19 whenever a Processor is added or replaced.

9.4 Professional Advisors. The Company discloses Personal Information to its attorneys, accountants, auditors, insurers, and other professional advisors, each of whom is bound by professional or contractual obligations of confidentiality, to the extent necessary for those advisors to render services to the Company.

9.5 Legal Disclosures. The Company discloses Personal Information when the Company believes in good faith that disclosure is required by applicable law, regulation, subpoena, court order, warrant, or other legal process, or by a lawful request of a governmental or regulatory authority; or when disclosure is reasonably necessary to enforce this Policy or the Terms of Use, to protect the rights, property, or safety of the Company, Individuals, Partner Clinics, or the public, or to detect, prevent, or address fraud, security, or technical issues. Where permitted by law and where practicable, the Company will notify the affected Individual of a compelled disclosure of Consumer Health Data before making it, and will disclose only the minimum information required. The Company will challenge any request for Consumer Health Data that it considers overbroad or improper to the extent it has a good-faith basis to do so.

9.6 Corporate Transactions. If the Company is involved in a merger, acquisition, financing, reorganization, bankruptcy, receivership, dissolution, sale or transfer of all or a portion of its assets, or similar transaction, Personal Information may be disclosed to the counterparty and its advisors in connection with due diligence, subject to confidentiality obligations, and may be transferred to the successor entity upon consummation. Any successor will be bound by this Policy with respect to Personal Information collected under it until the successor provides notice and, where applicable law requires, obtains consent under Article 19. Consumer Health Data will not be transferred in such a transaction to any entity that does not agree in writing to the restrictions in Article 8.2.

9.7 Affiliates. The Company has no parent company, subsidiary, or affiliate as of the Effective Date. If the Company forms or acquires an affiliate, Personal Information may be disclosed to that affiliate only for the purposes described in Article 8 and subject to this Policy, and Appendix C will be updated accordingly.

9.8 With Consent or at the Individual's Direction. The Company discloses Personal Information to any other recipient when the Individual has directed the Company to do so or has given consent to the specific disclosure.

9.9 Remedial Steps. If the Company learns that a Partner Clinic or Processor has Processed Personal Information in a manner inconsistent with this Policy or the applicable contract, the Company will (a) require the recipient to cease the non-compliant Processing; (b) require the recipient to remediate and, where appropriate, delete the affected information; (c) suspend further disclosures to the recipient pending remediation; (d) terminate the relationship where the recipient fails to remediate; and (e) notify affected Individuals where required by applicable law or where the Company determines that notification is warranted.

9.10 De-identified and Aggregated Data. The Company may create De-identified Data and Aggregated Data from Personal Information and may use and disclose such data for any lawful purpose, including publishing statistics concerning the geographic distribution of interest in the Saccade Assessment. The Company commits, in accordance with Cal. Civ. Code Section 1798.140(m) and equivalent provisions of other applicable state privacy laws, that it (a) will maintain and use such data only in de-identified or aggregated form; (b) will not attempt to re-identify any Individual from such data; and (c) will contractually obligate any recipient to comply with the same commitments.

ARTICLE 10. COOKIES, ANALYTICS, SESSION REPLAY, AND TRACKING SIGNALS

10.1 Cookies Used. The Site sets the following cookies and similar technologies, and no others:

- (a) a strictly necessary, first-party cookie named "saccade_consent," which records the Individual's cookie preferences and consent selections, persists for twelve months, and is exempt from consent requirements as strictly necessary to honor the Individual's choices;
- (b) first-party analytics cookies and local-storage entries set by the PostHog script, including a cookie named with the prefix "ph_" that contains a randomly generated identifier used to recognize repeat visits from the same browser, which persist for twelve months and are set only after the Individual has accepted analytics cookies through the consent banner described in Section 10.2, except in jurisdictions where applicable law permits such cookies to be set on an opt-out basis, in which case they are set at the first page load and may be disabled at any time through the banner; and
- (c) session cookies set by Vercel that are strictly necessary for load balancing and for serving the Site and that expire when the browser session ends.

10.2 Consent Banner. On the first visit from a browser, the Site displays a banner that describes the cookies in Section 10.1, offers the Individual the choice to accept or decline analytics cookies with equal prominence, and provides a link to this Article. The Individual's selection is recorded in the "saccade_consent" cookie and may be changed at any time through the "Cookie preferences" link in the Site footer.

10.3 Session Replay. When analytics cookies are enabled, the PostHog script records Site interactions in a form that may be replayed by the Company's staff to observe how Visitors navigate the Site. The Company has configured session replay so that (a) the content of every input, textarea, and select element on every form is masked at the point of capture and is replaced by placeholder characters before transmission, so that no name, email address, telephone number, ZIP code, age, selection, or response to the Optional Health Question is ever recorded in a session replay; (b) all text content within elements bearing the "ph-no-capture" attribute, which the Company applies to every form and every element displaying Personal Information, is excluded from capture; and (c) recordings are retained for the period stated in Article 13. Session replay does not capture keystrokes, clipboard content, or content of other browser tabs.

10.4 Internet Protocol Addresses. The Company has configured PostHog to derive an approximate city-level or region-level location from each Internet Protocol address and to discard the full address so that it is not stored in the analytics event record. Vercel server logs, which contain full Internet Protocol addresses, are retained for the period stated in Article 13 and are used only for the purposes in Section 8.1(f) and (g).

10.5 No Third-Party Advertising Technologies. The Site does not load, and the Company commits that it will not load, any advertising pixel, tag, software development kit, or script operated by an advertising network, social media platform, or data broker, including those operated by Meta Platforms, Inc., Google LLC (including Google Analytics and Google Ads), TikTok Inc., Microsoft Corporation (including Bing Ads and Clarity), Snap Inc., Pinterest, Inc., X Corp., LinkedIn Corporation, or any similar entity. The Company does not use retargeting, lookalike audiences, customer-match audiences, or conversion application programming interfaces.

10.6 Global Privacy Control and Opt-Out Preference Signals. The Site recognizes and honors the Global Privacy Control signal and any other opt-out preference signal recognized by applicable law, including as required by Cal. Civ. Code Section 1798.135(b), Colo. Rev. Stat. Section 6-1-1306(1)(a)(IV), and Conn. Gen. Stat. Section 42-520(e). Because the Company does not Sell or Share Personal Information and does not engage in Targeted Advertising, honoring such a signal has no effect on the Company's Processing beyond that already provided by this Policy; nevertheless, when the Site detects such a signal, it treats the signal as a decline of analytics cookies under Section 10.2 for that browser and records that treatment in the "saccade_consent" cookie.

10.7 Do Not Track. The Site treats a browser "Do Not Track" header in the same manner as a Global Privacy Control signal under Section 10.6.

10.8 Browser Controls. An Individual may block or delete cookies through browser settings. Blocking the "saccade_consent" cookie will cause the consent banner to reappear on each visit. Blocking all other cookies described in Section 10.1 does not impair the functionality of the Site or the forms.

ARTICLE 11. COMMUNICATIONS, MARKETING, AND TELEPHONE CONSENT

11.1 Transactional Communications. The Company sends the transactional communications described in Section 8.1(d) to every Registrant and Applicant. These communications are necessary to the Services requested and may not be opted out of while the Individual remains enrolled in the applicable program; withdrawal from the program under Section 5.6 or 6.5 ends them.

11.2 Informational Communications. The Company sends the informational communications described in Section 8.1(e) only to Individuals who have given the Contact Consent. Every such communication sent by email contains a functioning unsubscribe mechanism that takes effect within ten business days as required by the CAN-SPAM Act, 15 U.S.C. Section 7701 et seq., and identifies the Company as the sender with a valid physical postal address as required by 16 C.F.R. Section 316.5. The Company does not send informational communications on behalf of any third party and does not permit any third party to send communications to Individuals on the Company's behalf other than the Processors in Section 9.3.

11.3 Telephone Calls. If an Individual provides a telephone number, the Company may place live, non-automated telephone calls to that number for the purposes in Section 8.1(a) through (d). The Company does not place calls using an automatic telephone dialing system or an artificial or prerecorded voice within the meaning of the Telephone Consumer Protection Act, 47 U.S.C. Section 227 ("TCPA"). The Company honors the National Do Not Call Registry and its own internal do-not-call list, and adds any Individual who requests not to be called to that list within three business days.

11.4 SMS Messages. The Company does not send SMS messages as of the Effective Date. If the Company begins to send SMS messages, it will do so only (a) to Individuals who have given prior express written consent within the meaning of 47 C.F.R. Section 64.1200(f)(9) through a separate, clearly labeled opt-in that

discloses the sender, the nature and approximate frequency of messages, that message and data rates may apply, and the means of opting out; (b) with the words "Reply STOP to opt out" or an equivalent instruction in the first message and at reasonable intervals thereafter; (c) honoring any opt-out request within ten business days as required by 47 C.F.R. Section 64.1200(a)(10); and (d) after updating Appendix A and Appendix C under Article 19. SMS consent will never be a condition of participation in any program.

11.5 Communications Preferences. An Individual may change communication preferences at any time by the means described in Article 14.9.

ARTICLE 12. SECURITY

12.1 Standard of Care. The Company maintains an information security program containing administrative, technical, and physical safeguards that are reasonable and appropriate to the size and complexity of the Company, the nature and scope of its activities, and the sensitivity of the Personal Information it Processes, as required by Section 5 of the Federal Trade Commission Act, Cal. Civ. Code Section 1798.81.5, Cal. Civ. Code Section 1798.150, and the security provisions of other applicable state privacy laws. The Company applies the safeguards in this Article to all Personal Information and applies the heightened safeguards in Section 12.3 to Consumer Health Data.

12.2 Technical and Organizational Measures. The Company's measures include: (a) encryption of Personal Information in transit using Transport Layer Security version 1.2 or higher, with plaintext connections to the Site refused; (b) encryption of Personal Information at rest in every database and backup using the Advanced Encryption Standard with 256-bit keys or a stronger standard; (c) row-level security policies on every database table containing Personal Information, such that no database query can return a record except through an authenticated and authorized path; (d) restriction of write access to the Company's databases to server-side application code holding a service credential that is never transmitted to any browser; (e) multi-factor authentication required for every staff account with access to any system containing Personal Information; (f) role-based access control under which access to Personal Information is granted only to named staff whose duties require it, is reviewed at least quarterly, and is revoked within one business day of the end of the staff member's need or employment; (g) logging of every access to, export of, and modification of Personal Information, with logs retained for the period in Article 13 and reviewed for anomalies at least monthly; (h) server-side validation of every form submission, rate limiting, and abuse detection to prevent automated or malicious submissions; (i) secure software development practices, including code review and dependency vulnerability scanning before deployment; (j) vendor due diligence under which every Processor is assessed for security posture before engagement and at least annually thereafter; (k) encrypted backups retained for the period in Article 13 with tested restoration procedures; (l) staff training on this Policy and on the handling of Consumer Health Data upon hiring and at least annually; and (m) a written incident response plan, tested at least annually, that assigns responsibilities for detection, containment, assessment, notification, and remediation.

12.3 Heightened Safeguards for Consumer Health Data. In addition to the measures in Section 12.2, the Company (a) stores each response to the Optional Health Question in a database column separate from other fields, subject to a distinct access policy under which fewer staff members have read access than to the remainder of the record; (b) excludes the response from every automated notification, export, report, and analytics event; (c) excludes the response from every communication with a Partner Clinic except the single disclosure described in Section 5.3(g); and (d) applies the shorter retention period stated in Article 13.

12.4 Limitations. No method of transmission over the Internet and no method of electronic storage is completely secure. The Company cannot guarantee absolute security, and Individuals acknowledge that they provide Personal Information at their own risk to the extent permitted by applicable law. This Section does not limit any obligation the Company owes under applicable law and does not limit the Company's commitments in Sections 12.1 through 12.3.

12.5 Security Incident Notification. If the Company determines that a security incident has resulted in the unauthorized acquisition of, or access to, unencrypted Personal Information, the Company will (a) contain the incident; (b) assess its scope and the Individuals affected; (c) notify affected Individuals without unreasonable delay and within the time required by the applicable state breach notification law, including Cal. Civ. Code Section 1798.82, and by 16 C.F.R. Part 318 to the extent applicable, by email to the address on file or by another method permitted by law; (d) notify the applicable state attorneys general, the Federal Trade Commission, and other regulators as required by law; (e) notify any affected Partner Clinic as required by the applicable Business Associate Agreement; and (f) document the incident, the Company's response, and the measures taken to prevent recurrence. Notification will describe the nature of the incident, the categories of Personal Information involved, the steps the Company has taken, the steps the Individual may take, and how to contact the Company.

12.6 Reporting Vulnerabilities. Any person who believes he or she has discovered a security vulnerability in the Site may report it to security@saccade.com. The Company will acknowledge the report within five business days and will not pursue legal action against a good-faith researcher who complies with applicable law, does not access or modify Personal Information beyond what is necessary to demonstrate the vulnerability, and gives the Company a reasonable opportunity to remediate before public disclosure.

ARTICLE 13. DATA RETENTION

13.1 Principle. The Company retains Personal Information only for as long as reasonably necessary to fulfill the purposes for which it was collected, to comply with legal obligations, to resolve disputes, and to enforce agreements, and in no event longer than the periods stated in this Article, unless a longer period is required by law or by a litigation hold.

13.2 Retention Schedule. The Company applies the following retention periods, which are reproduced with additional detail in Appendix D:

- (a) Patient Interest Submissions, excluding the response to the Optional Health Question: until the earlier of (i) twelve months after the Registrant is introduced to a Partner Clinic under Section 5.2, or (ii) twenty-four months after the date of submission if no introduction has occurred; and in every case, deletion within the period in Article 14.10 upon the Registrant's request or withdrawal;
- (b) response to the Optional Health Question: until the earlier of (i) the introduction of the Registrant to a Partner Clinic under Section 5.2, immediately after which the response is deleted from the Company's systems, or (ii) twelve months after the date of submission if no introduction has occurred; and in every case, deletion within the period in Article 14.10 upon withdrawal of the Health Data Consent;
- (c) Clinic Partner Applications: for the duration of the Partner Clinic relationship and for thirty-six months thereafter, or twenty-four months after the date of submission if no Partner Clinic Agreement is executed;

- (d) consent records, including the text of the consent presented, the selection made, and the date, time, and Internet Protocol address of the selection: for as long as the Personal Information to which the consent relates is retained, and for thirty-six months thereafter, as evidence of compliance;
- (e) records of requests under Article 14 and the Company's responses: twenty-four months from the date of the response, as required by Cal. Code Regs. tit. 11, Section 7101(a);
- (f) analytics event data: twelve months from the date of collection, after which it is deleted or converted to Aggregated Data;
- (g) session replay recordings: thirty days from the date of recording;
- (h) server logs containing Internet Protocol addresses: ninety days from the date of the request;
- (i) access and audit logs described in Section 12.2(g): twenty-four months from the date of the logged event;
- (j) email correspondence with Individuals: thirty-six months from the date of the last message in the thread, unless the correspondence relates to a request under Article 14, a security incident, or a legal matter, in which case the period in (e), (k), or (l) applies;
- (k) security incident records: seventy-two months from the date the incident is closed;
- (l) records subject to a litigation hold or a governmental inquiry: until the hold is released by the Company's legal counsel; and
- (m) encrypted backups: thirty-five days on a rolling basis, after which each backup is overwritten, such that any record deleted from the production database is absent from every backup within thirty-five days of deletion.

13.3 Method of Deletion. Upon expiry of a retention period or upon a deletion request, the Company deletes Personal Information by permanently erasing it from the production database and, where the Company is unable to erase it from an archival system within the period required, by rendering it permanently inaccessible and unusable until it is overwritten under Section 13.2(m). The Company instructs each Processor to delete or return the corresponding Personal Information and obtains confirmation of deletion.

ARTICLE 14. RIGHTS OF INDIVIDUALS AND HOW TO EXERCISE THEM

14.1 Rights Available to Every Individual. Regardless of the Individual's state or country of residence, and whether or not any law grants the right, the Company extends to every Individual the following rights with respect to Personal Information the Company holds about the Individual:

- (a) the right to confirm whether the Company is Processing the Individual's Personal Information and to access that information;
- (b) the right to receive a copy of the Personal Information the Individual provided to the Company in a portable and, to the extent technically feasible, readily usable format;
- (c) the right to correct inaccurate Personal Information;
- (d) the right to delete Personal Information;

- (e) the right to withdraw any consent previously given;
- (f) the right to opt out of informational communications;
- (g) the right to know the categories of Personal Information the Company has collected, the categories of sources, the purposes of collection, the categories of third parties to whom the Company has disclosed Personal Information, and the specific pieces of Personal Information collected, which information is provided in Articles 4, 8, and 9 and Appendix B and may be requested in individualized form;
- (h) the right not to be discriminated against, denied goods or services, charged a different price, or provided a different level of service for exercising any right; and
- (i) the right to appeal a decision of the Company concerning a request, as described in Section 14.12.

14.2 Rights Concerning Consumer Health Data. In addition to the rights in Section 14.1, every Individual has the following rights with respect to Consumer Health Data, in accordance with Wash. Rev. Code Section 19.373.040 and equivalent laws: (a) the right to confirm whether the Company is collecting, sharing, or Selling Consumer Health Data concerning the Individual and to access that data, including a list of all third parties and affiliates with whom the Company has shared or to whom it has Sold the data, and an active email address or other online mechanism for contacting each such third party; (b) the right to withdraw consent to the collection and sharing of Consumer Health Data; and (c) the right to have Consumer Health Data deleted, including from the Company's archives, backups, and Processors, and to have the Company notify every third party with whom the data was shared of the deletion request. The Company does not Sell Consumer Health Data and therefore no valid authorization under Wash. Rev. Code Section 19.373.070 exists or is sought.

14.3 California Residents. Residents of California have the rights in Sections 14.1 and 14.2 and the following additional rights and disclosures under the CCPA: (a) the right to limit the use and disclosure of Sensitive Personal Information under Cal. Civ. Code Section 1798.121, which the Company satisfies in advance by using Sensitive Personal Information, consisting of the response to the Optional Health Question, only for the purposes permitted by Cal. Code Regs. tit. 11, Section 7027(m) and the purpose for which it was provided, so that no "Limit the Use of My Sensitive Personal Information" link is required; (b) the right to opt out of the Sale or Sharing of Personal Information under Cal. Civ. Code Section 1798.120, which the Company does not engage in, so that no "Do Not Sell or Share My Personal Information" link is required; (c) notice that the Company does not offer financial incentives or price or service differences in exchange for the retention or Sale of Personal Information; (d) notice that the Company does not have actual knowledge that it Sells or Shares the Personal Information of consumers under sixteen years of age; (e) the disclosures required by Cal. Civ. Code Section 1798.130(a)(5), which are set forth in Appendix B; (f) notice, under Cal. Civ. Code Section 1798.83, that the Company does not disclose Personal Information to third parties for their direct marketing purposes; (g) the right to designate an authorized agent under Section 14.8; and (h) the Notice at Collection required by Cal. Civ. Code Section 1798.100(a), which is set forth in Appendix E and is presented at or before the point of collection on each form.

14.4 Residents of Other States with Comprehensive Privacy Laws. Residents of Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia have the rights in Sections 14.1 and 14.2 and the following additional rights under their respective laws: (a) the right to opt out of Targeted Advertising, the Sale of personal data, and profiling in furtherance of decisions that produce legal or

similarly significant effects, none of which the Company engages in; (b) the right to obtain a list of the specific third parties to which the Company has disclosed the Individual's personal data, where the applicable law so provides, including under Or. Rev. Stat. Section 646A.574(1)(b), Minn. Stat. Section 325O.05, and Del. Code Ann. tit. 6, Section 12D-104(a)(1); (c) with respect to Sensitive Personal Information, the right to have it Processed only with consent, which the Company satisfies through the Health Data Consent; (d) with respect to Maryland residents, notice that the Company collects Sensitive Personal Information consisting of the response to the Optional Health Question only where strictly necessary to provide the service requested, in accordance with Md. Code Ann., Com. Law Section 14-4607(a)(2), and does not Sell it under any circumstances; (e) with respect to Minnesota residents, the right to question the result of any profiling, which the Company does not conduct for decisions producing legal or similarly significant effects, and the right to obtain the Company's documented data inventory, which is Appendix B; and (f) the right to appeal under Section 14.12. The Company applies the requirements of each such law to its residents whether or not the Company meets that law's applicability thresholds, and the Company's applicability under each such law is reassessed annually.

14.5 Nevada Residents. The Company does not Sell covered information as defined in Nev. Rev. Stat. Section 603A.340 and does not Sell Consumer Health Data as defined in Nevada Senate Bill 370. Nevada residents may nonetheless submit a request to opt out of any future Sale by the means in Section 14.9, and the Company will honor such a request should its practices ever change.

14.6 Washington Residents and Individuals Whose Consumer Health Data Is Collected in Washington. This Policy, and in particular Articles 2, 4, 5, 8, 9, 12, 13, and 14 and Appendices A through D, together constitute the Consumer Health Data Privacy Policy required by Wash. Rev. Code Section 19.373.020. The categories of Consumer Health Data collected are stated in Section 2.7; the purposes are stated in Article 8; the sources are stated in Article 4; the categories of third parties and affiliates with which Consumer Health Data is shared are stated in Article 9; and the means of exercising rights are stated in Sections 14.9 through 14.12. The Company does not implement a geofence within the meaning of Wash. Rev. Code Section 19.373.080 around any facility that provides in-person health care services.

14.7 Individuals in the European Economic Area, the United Kingdom, and Switzerland. The Company is established solely in the United States, does not offer goods or services to, and does not monitor the behavior of, individuals in the European Economic Area, the United Kingdom, or Switzerland, and has not appointed a representative under GDPR Article 27. If, notwithstanding the foregoing, the GDPR, the UK General Data Protection Regulation, or the Swiss Federal Act on Data Protection applies to any Processing, the Individual has the rights of access, rectification, erasure, restriction, portability, and objection, and the right not to be subject to a decision based solely on automated processing, under Articles 15 through 22 of the GDPR and their equivalents; the legal bases in Section 8.3 apply; Personal Information is transferred to and Processed in the United States on the basis of the Individual's explicit consent under GDPR Article 49(1)(a) after being informed of the risks, or, where the Company has executed Standard Contractual Clauses with the relevant Processor, on the basis of those clauses under GDPR Article 46(2)(c); and the Individual has the right to lodge a complaint with the supervisory authority of the Individual's habitual residence, place of work, or place of the alleged infringement.

14.8 Authorized Agents. An Individual may designate an authorized agent to submit a request on the Individual's behalf. The Company will require the agent to provide written authorization signed by the Individual, or a copy of a power of attorney valid under Cal. Prob. Code Sections 4121 to 4130 or equivalent law, and may require the Individual to verify his or her own identity directly with the Company and to confirm that the agent has been authorized, except where a power of attorney has been provided. A parent or

legal guardian may submit a request on behalf of a minor, and a court-appointed conservator or guardian may submit a request on behalf of an adult, upon providing evidence of that status.

14.9 How to Submit a Request. An Individual may submit any request under this Article, exercise any choice, or withdraw any consent by any of the following methods: (a) by email to privacy@saccade.com; (b) through the web form located at saccade.com/privacy-request; (c) by using the unsubscribe link in any informational email, for opt-out requests; or (d) by postal mail addressed to Saccade, Inc., Attention: Privacy Officer, at the principal office address stated on the "Contact" page of the Site. Requests need not be in any particular form and need not cite any law. The Company will not require an Individual to create an account to submit a request.

14.10 Verification and Response Timelines. The Company will confirm receipt of a request within ten business days and will respond substantively within forty-five days of receipt. Where reasonably necessary, taking into account the complexity and number of requests, the Company may extend that period by up to forty-five additional days, in which case the Company will notify the Individual of the extension and the reason within the initial forty-five-day period. The Company verifies requests by matching the information provided with the information on file, ordinarily by sending a confirmation link to the email address on file; for requests to access specific pieces of Personal Information or to delete, the Company requires confirmation from the email address on file and may request one additional data point present in the record, such as the ZIP code. The Company does not require government-issued identification and does not retain any information collected solely for verification beyond the period in Section 13.2(e). Where the Company cannot verify a request, it will inform the Individual and, for a request to know categories of Personal Information, will respond with the general disclosures in this Policy. Requests for deletion of Consumer Health Data are fulfilled, and every Processor and Partner Clinic that received the data is notified, within thirty days of verification, and in every case within the period required by Wash. Rev. Code Section 19.373.040(3).

14.11 Fees and Limits. The Company does not charge a fee for responding to requests. If requests from an Individual are manifestly unfounded, excessive, or repetitive, the Company may charge a reasonable fee reflecting the administrative cost or decline to act, in which case the Company will explain the basis for its decision and the Individual may appeal under Section 14.12. The Company will respond to no fewer than two requests for access from the same Individual in any twelve-month period without charge.

14.12 Appeals. If the Company declines to take action on a request, in whole or in part, it will inform the Individual in writing of the reasons and of the right to appeal. An Individual may appeal by replying to the Company's decision, by email to privacy@saccade.com with the subject line "Appeal," or by the postal method in Section 14.9, within sixty days of receiving the decision. The Company's Privacy Officer, or a member of staff who was not involved in the original decision, will review the appeal and respond in writing within forty-five days of receipt, or within sixty days for Colorado and Virginia residents where the applicable law so permits and the Company notifies the Individual of the extension, stating the action taken or the reasons for declining and, where the appeal is denied, providing the means by which the Individual may contact the attorney general of the Individual's state of residence to submit a complaint, including the following: California Privacy Protection Agency, cpa.ca.gov; Colorado Attorney General, coag.gov; Connecticut Attorney General, portal.ct.gov/ag; Delaware Department of Justice, attorneygeneral.delaware.gov; Indiana Attorney General, in.gov/attorneygeneral; Iowa Attorney General, iowaattorneygeneral.gov; Kentucky Attorney General, ag.ky.gov; Maryland Attorney General, marylandattorneygeneral.gov; Minnesota Attorney General, ag.state.mn.us; Montana Attorney General, dojmt.gov; Nebraska Attorney General, ago.nebraska.gov; New Hampshire Attorney General, doj.nh.gov;

New Jersey Attorney General, njoag.gov; Oregon Attorney General, doj.state.or.us; Rhode Island Attorney General, riag.ri.gov; Tennessee Attorney General, tn.gov/attorneygeneral; Texas Attorney General, texasattorneygeneral.gov; Utah Attorney General, attorneygeneral.utah.gov; Virginia Attorney General, oag.state.va.us; and Washington Attorney General, atg.wa.gov.

14.13 Records. The Company maintains a record of every request received, the date received, the nature of the request, the manner of response, the date of response, and the basis for any denial, for the period in Section 13.2(e), and compiles the metrics required by Cal. Code Regs. tit. 11, Section 7102 if and when the Company meets the threshold in that section.

ARTICLE 15. CHILDREN AND MINORS

15.1 Minimum Age. The Site and the Services are directed to adults aged eighteen years and older. The Company does not knowingly collect Personal Information from any Individual under eighteen years of age, and the age field on the Patient Interest Form rejects any value below eighteen at the point of entry.

15.2 Children Under Thirteen. The Company does not knowingly collect Personal Information from children under thirteen years of age and does not direct any part of the Site to children, within the meaning of the Children's Online Privacy Protection Act, 15 U.S.C. Section 6501 et seq., and 16 C.F.R. Part 312.

15.3 Remediation. If the Company learns that it has collected Personal Information from an Individual under eighteen years of age without the verifiable consent of a parent or legal guardian where such consent would be required, the Company will delete that information within ten business days. A parent or guardian who believes that a minor has provided Personal Information to the Company may contact the Company by the means in Section 14.9.

15.4 Inquiries on Behalf of Minors. The Patient Interest Form may be submitted only by an adult and only on behalf of the adult submitting it or another adult. The "Someone else" option on the form is not intended for, and the Saccade Assessment is not intended for, any person under eighteen years of age.

ARTICLE 16. INTERNATIONAL VISITORS AND CROSS-BORDER TRANSFERS

16.1 Location of Processing. The Company is located in the United States and Processes and stores all Personal Information in the United States, using the Processors identified in Appendix C, each of which stores Personal Information on infrastructure located in the United States.

16.2 Transfers from Other Jurisdictions. If an Individual accesses the Site from outside the United States, the Individual's Personal Information will be transferred to, stored in, and Processed in the United States, where privacy laws may differ from and may be less protective than those of the Individual's jurisdiction. By providing Personal Information to the Company, an Individual located outside the United States acknowledges that transfer. Where applicable law requires a specific transfer mechanism, the Company relies on the mechanisms in Section 14.7.

16.3 Canada. To the extent the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, or a substantially similar provincial law applies, the Company Processes Personal Information with the knowledge and consent of the Individual, limits collection to what is necessary for the identified purposes, and provides access and correction rights, all as described in this Policy. Individuals in Canada may direct complaints to the Office of the Privacy Commissioner of Canada.

ARTICLE 17. THIRD-PARTY SITES AND SERVICES

17.1 Links. The Site may contain links to websites and services operated by third parties, including Partner Clinics, Y Combinator Management, LLC, research publishers, and social media platforms. The Company does not control those websites or services, this Policy does not apply to them, and the Company is not responsible for their content or privacy practices. Individuals should review the privacy policy of every third-party website or service before providing Personal Information to it.

17.2 Embedded Content. The Site does not embed third-party content that sets cookies or collects Personal Information, including embedded video players, social media widgets, chat widgets, or maps, as of the Effective Date. If the Company embeds such content in the future, it will do so only after updating Article 10 and Appendix C under Article 19 and, where required, obtaining consent through the banner described in Section 10.2.

ARTICLE 18. AUTOMATED DECISION-MAKING AND PROFILING

18.1 No Solely Automated Decisions with Significant Effects. The Company does not make any decision concerning an Individual based solely on automated Processing, including profiling, that produces legal effects concerning the Individual or similarly significantly affects the Individual, within the meaning of GDPR Article 22, Cal. Civ. Code Section 1798.185(a)(16), Colo. Rev. Stat. Section 6-1-1306(1)(a)(I)(C), and equivalent provisions. The prioritization described in Section 5.5 is reviewed by a human before any action is taken and affects only the sequence of outreach.

18.2 No Automated Assessment through the Site. The Site does not administer the Saccade Assessment, does not compute any risk score, index, or classification concerning any Individual, and does not display any such output to any Individual. Any assessment output is generated only within the Partner Clinic environment described in Article 7 and is governed by that Article.

18.3 Risk Assessments. The Company conducts and documents a data protection assessment, in accordance with Cal. Civ. Code Section 1798.185(a)(15), Colo. Rev. Stat. Section 6-1-1309, Conn. Gen. Stat. Section 42-522, Va. Code Ann. Section 59.1-580, and equivalent provisions, before commencing any Processing of Sensitive Personal Information and before any material change to such Processing, and will make such assessments available to the applicable attorney general upon lawful request.

ARTICLE 19. AMENDMENT OF THIS POLICY

19.1 Right to Amend. The Company may amend this Policy from time to time to reflect changes in its practices, in applicable law, or in the Services. Each amendment will be identified by a new version number and a new effective date at the head of the Policy, and the Company will maintain each superseded version and a summary of changes in Appendix F and will make superseded versions available upon request under Section 14.9.

19.2 Notice of Amendments. The Company will post each amended Policy on the Site at least thirty days before its effective date, with the words "Updated Privacy Policy" and the new effective date displayed prominently on the Site's home page during that period, and will send notice of the amendment by email to every Registrant and Applicant whose Personal Information the Company then holds, except for amendments that are purely clerical, that add a Processor performing an existing function, or that expand the rights of Individuals, which take effect upon posting.

19.3 Material Changes Requiring Consent. If an amendment would (a) permit any new use or disclosure of Consumer Health Data; (b) permit any Sale or Sharing of Personal Information; (c) permit Targeted Advertising; (d) extend any retention period in Article 13; or (e) otherwise materially reduce the protections afforded to Personal Information collected under a prior version, the amendment will not apply to Personal Information collected under the prior version unless and until the Company has obtained the affirmative consent of the Individual to whom that information relates. Absent such consent, the prior version continues to govern that information.

19.4 Continued Use. Continued use of the Site after the effective date of an amendment that does not require consent under Section 19.3 constitutes acknowledgment of the amended Policy, provided that the Company has given the notice required by Section 19.2.

ARTICLE 20. GENERAL PROVISIONS

20.1 Governing Law. This Policy and any dispute arising out of or relating to it are governed by the laws of the State of California and the federal laws of the United States, without regard to conflict-of-law principles, except to the extent that the privacy law of the state or country of an Individual's residence mandatorily applies to the Processing of that Individual's Personal Information, in which case that law applies to the extent of the conflict. Nothing in this Section deprives an Individual of the protection of mandatory provisions of the law of the Individual's residence.

20.2 Severability. If any provision of this Policy is held invalid, illegal, or unenforceable in any jurisdiction, that provision shall be deemed modified to the minimum extent necessary to make it valid and enforceable in that jurisdiction, and the remaining provisions shall remain in full force and effect. The invalidity of a provision in one jurisdiction shall not affect its validity in any other jurisdiction.

20.3 No Waiver. The Company's failure to enforce any provision of this Policy shall not constitute a waiver of that provision or of any other provision. No waiver is effective unless in writing and signed by an authorized officer of the Company.

20.4 Entire Statement of Practices. This Policy, together with the Appendices, which are incorporated by reference and form part of this Policy, constitutes the complete statement of the Company's practices with respect to Personal Information within its scope, and supersedes every prior statement, representation, or notice concerning those practices, whether oral or written. No employee, contractor, or agent of the Company has authority to make any representation concerning the Company's privacy practices that is inconsistent with this Policy, and no such representation shall bind the Company.

20.5 Language. This Policy is written in English. Any translation is provided for convenience only, and in the event of any inconsistency, the English version controls.

20.6 Accessibility. The Company makes this Policy available in a format accessible to Individuals with disabilities, including by providing a screen-reader-compatible version on the Site and, upon request under Section 14.9, a large-print or plain-text version at no charge.

20.7 Assignment. The Company may assign its rights and obligations under this Policy to a successor in connection with a transaction described in Section 9.6, subject to the conditions in that Section. Individuals may not assign their rights under this Policy, which are personal to them, except through an authorized agent under Section 14.8.

20.8 Survival. Articles 7, 9.10, 12, 13, 14, and 20, and every commitment in this Policy expressed as continuing, survive any termination of an Individual's relationship with the Company and any amendment of this Policy to the extent provided in Section 19.3.

ARTICLE 21. CONTACT INFORMATION

21.1 Privacy Officer. The Company has designated a Privacy Officer who is responsible for the Company's compliance with this Policy and applicable privacy law and who may be contacted at privacy@saccade.com.

21.2 Contact Methods. Individuals may contact the Company concerning this Policy, their Personal Information, or any privacy concern by any of the following methods: (a) email to privacy@saccade.com; (b) the web form at saccade.com/privacy-request; (c) postal mail to Saccade, Inc., Attention: Privacy Officer, at the principal office address stated on the "Contact" page of the Site; or (d) security matters, email to security@saccade.com.

21.3 Complaints. An Individual who is dissatisfied with the Company's handling of a privacy matter may, in addition to the appeal in Section 14.12, submit a complaint to the Federal Trade Commission at reportfraud.ftc.gov, to the attorney general of the Individual's state of residence at the address listed in Section 14.12, or, where applicable, to the supervisory authority identified in Section 14.7 or 16.3.

APPENDIX A. CONSENT LANGUAGE AND FORM SPECIFICATIONS

A.1 Patient Interest Form. The Patient Interest Form presents the following fields in the following order. Fields marked "Required" must be completed to submit the form. Fields marked "Optional" may be left blank without effect on submission.

Field	Type	Status
First name	Text	Required
Email address	Email	Required
Phone number	Telephone	Optional
ZIP code	Five-digit numeric	Required
Age	Numeric, 18 to 110	Required
Who is the test for?	Single selection: Me; A parent; A spouse or partner; Someone else	Required
How did you hear about us?	Single selection: Doctor; Friend or family; Search; Social; News; Other	Optional
Have you or the person this is for noticed any memory or thinking changes?	Single selection: No; Not sure; Yes, mild; Yes, noticeable; Prefer not to say	Optional
Contact Consent	Checkbox, unchecked by default	Required
Health Data Consent	Checkbox, unchecked by default; displayed only when the preceding question has been answered	Required only if the preceding question has been answered

A.2 Contact Consent Text (Patient Interest Form). The Contact Consent checkbox is accompanied by the following text, verbatim: "I agree that Saccade may contact me by email, and by phone if I have provided a number, about the availability of Saccade screening near me. I have read the Privacy Policy. I understand that Saccade is not a healthcare provider, that submitting this form does not create a patient relationship, and

that I can withdraw this consent at any time."

A.3 Health Data Consent Text. The Health Data Consent checkbox is accompanied by the following text, verbatim: "I consent to Saccade collecting my answer to the question about memory and thinking changes, storing it as described in the Privacy Policy, and sharing it with the one clinic I choose to be introduced to, for the sole purpose of arranging a screening. This answer is health information. I understand that I did not have to answer the question, that I can withdraw this consent at any time by emailing privacy@saccade.com, and that withdrawing will delete my answer."

A.4 Patient Interest Form Notice at Collection. Immediately above the submit button, the Patient Interest Form displays the following text, verbatim: "We collect the information on this form to match you with a Saccade partner clinic and to tell you when one is available near you. We keep it for up to 24 months, or 12 months after we introduce you to a clinic. We never sell it and never use it for advertising. Full details, including your rights, are in our Privacy Policy."

A.5 Clinic Partner Application. The Clinic Partner Application presents the following fields in the following order.

Field	Type	Status
Your name	Text	Required
Role	Single selection: Physician; Practice owner; Practice manager; Other	Required
Work email	Email	Required
Phone	Telephone	Optional
Clinic name	Text	Required
Clinic website	URL	Optional
City and state	Text	Required
Practice type	Single selection: Longevity or preventive; Neurology; Primary care; Concierge; Other	Required
Patients seen per month	Single selection: Under 100; 100 to 500; 500 to 2,000; 2,000 or more	Required
Cognitive or biomarker screening offered today	Single selection: None; Cognitive tests; Blood biomarkers; Imaging; Several	Required
Number of locations	Single selection: 1; 2 to 5; 6 or more	Optional
Why Saccade for your practice?	Text, 300 characters maximum	Optional
Contact Consent	Checkbox, unchecked by default	Required

A.6 Contact Consent Text (Clinic Partner Application). The Contact Consent checkbox is accompanied by the following text, verbatim: "I agree that Saccade may contact me about this application by email and, if I have provided a number, by phone. I confirm that I am authorized to submit this application on behalf of the clinic named above. I have read the Privacy Policy."

A.7 Clinic Partner Application Notice at Collection. Immediately above the submit button, the Clinic Partner Application displays the following text, verbatim: "We collect the information on this form to evaluate your clinic for the Saccade launch program and to contact you about next steps. We keep it for 24 months if no partnership results. We never sell it. Full details are in our Privacy Policy."

APPENDIX B. CALIFORNIA DISCLOSURES: CATEGORIES OF PERSONAL INFORMATION

B.1 The following table sets forth, for each category of Personal Information enumerated in Cal. Civ. Code Section 1798.140(v), whether the Company has collected it in the twelve months preceding the Effective Date and collects it currently, the sources, the purposes, and the categories of recipients to which it has been disclosed for a business purpose. The Company has not Sold or Shared any category.

Category (Cal. Civ. Code 1798.140(v))	Collected	Sources	Purposes (Article 8)	Disclosed to (Article 9)
A. Identifiers: name, email, telephone, IP address, cookie identifier	Yes	Individual; automatic collection	8.1(a) to (i)	Partner Clinic (name, email, phone only, upon confirmation); Processors
B. Categories in Cal. Civ. Code 1798.80(e): name, telephone	Yes	Individual	8.1(a) to (e)	Partner Clinic (upon confirmation); Processors
C. Protected classifications: age	Yes	Individual	8.1(a), (j)	Partner Clinic (upon confirmation); Processors
D. Commercial information	No	None	None	None
E. Biometric information	No	None	None	None
F. Internet or network activity: pages viewed, interactions, referrer	Yes	Automatic collection	8.1(f), (g)	Processors (PostHog, Vercel)
G. Geolocation data: ZIP code; city-level location from IP	Yes	Individual; automatic collection	8.1(a), (f), (j)	Partner Clinic (ZIP only, upon confirmation); Processors
H. Sensory data	No	None	None	None
I. Professional or employment information: role, clinic name	Yes (Applicants only)	Individual; public registries	8.1(b)	Processors
J. Education information	No	None	None	None
K. Inferences: region, matching priority, clinic fit	Yes	Derived by Company	8.1(a), (b), (j)	None
L. Sensitive Personal Information: response to Optional Health Question	Yes, only with Health Data Consent	Individual	8.1(a)	Partner Clinic (upon confirmation and Health Data Consent); Processor (Supabase)

B.2 Retention. The retention period for each category is stated in Article 13 and Appendix D, by reference to the data element concerned.

B.3 Business Purposes for Disclosure. Disclosures to Processors are made for the business purposes enumerated in Cal. Civ. Code Section 1798.140(e), specifically: performing services on behalf of the Company, including maintaining accounts, providing customer service, processing requests, and providing analytic services; auditing related to compliance; ensuring security and integrity; debugging; and short-term transient use.

APPENDIX C. PROCESSORS

C.1 The following Processors are engaged as of the Effective Date. Each is bound by a written contract meeting the requirements of Section 9.3.

Processor	Function	Personal Information Processed	Location of Processing
Supabase, Inc.	Database hosting and storage	All form submissions, consent records, request records	United States
Vercel Inc.	Website hosting and content delivery	IP addresses, request logs, session cookies	United States, with edge caching of non-personal static assets globally
PostHog, Inc.	Product analytics and session replay	Automatically collected information under Article 4.2, with form content masked and IP addresses truncated	United States
Resend, Inc.	Transactional and informational email delivery	Name, email address, message content, delivery metadata	United States
Slack Technologies, LLC	Internal notifications	Form type, city and state, timestamp, record link; no name, contact detail, age, or health response	United States
Google LLC (Google Workspace)	Business email and document storage	Correspondence with Individuals; internal documents referencing Individuals	United States

C.2 No SMS Processor is engaged as of the Effective Date. Section 11.4 governs any future engagement.

C.3 No affiliate of the Company exists as of the Effective Date. Section 9.7 governs any future affiliate.

APPENDIX D. RETENTION SCHEDULE

Record	Retention Period	Trigger	Deletion Method
Patient Interest Submission (excluding health response)	12 months after introduction to Partner Clinic, or 24 months after submission if no introduction	Earlier of the two	Permanent erasure from production database; Processor deletion instruction; backup overwrite within 35 days
Response to Optional Health Question	Immediately upon introduction to Partner Clinic, or 12 months after submission if no introduction	Earlier of the two	Same as above, plus notification to any Partner Clinic that received it
Clinic Partner Application	Duration of partnership plus 36 months, or 24 months after submission if no agreement executed	End of partnership or submission date	Permanent erasure; Processor deletion instruction
Consent records	Life of the related Personal Information plus 36 months	Deletion of related record	Permanent erasure
Rights-request records	24 months after response	Date of response	Permanent erasure
Analytics event data	12 months	Date of collection	Deletion or conversion to Aggregated Data
Session replay recordings	30 days	Date of recording	Automatic deletion by Processor
Server logs with IP addresses	90 days	Date of request	Automatic deletion by Processor
Access and audit logs	24 months	Date of logged event	Permanent erasure
Email correspondence	36 months after last message	Date of last message	Permanent erasure
Security incident records	72 months after closure	Closure date	Permanent erasure
Records under litigation hold	Until release by legal counsel	Release of hold	Per applicable schedule above
Encrypted backups	35 days rolling	Backup creation	Overwrite

APPENDIX E. CALIFORNIA NOTICE AT COLLECTION

E.1 The following notice is presented at or before the point of collection on each form on the Site, in accordance with Cal. Civ. Code Section 1798.100(a) and Cal. Code Regs. tit. 11, Section 7012.

E.2 Categories collected on the Patient Interest Form: identifiers (name, email address, telephone number); protected classifications (age); geolocation data (ZIP code); inferences (region and matching priority); and, only with separate consent, Sensitive Personal Information (response to the question concerning memory and thinking changes). Purposes: to match the Individual with a partner clinic, to communicate availability, and to maintain required records. Retention: as stated in Appendix D. Sale or Sharing: none. Link to this Policy: saccade.com/privacy.

E.3 Categories collected on the Clinic Partner Application: identifiers (name, email address, telephone number); professional information (role, clinic name, clinic details). Purposes: to evaluate the application and communicate about the program. Retention: as stated in Appendix D. Sale or Sharing: none. Link to this Policy: saccade.com/privacy.

E.4 Categories collected automatically from all Visitors: identifiers (IP address, cookie identifier); internet or network activity; geolocation data (city-level, derived). Purposes: to operate, secure, and improve the Site. Retention: as stated in Appendix D. Sale or Sharing: none. Link to this Policy: saccade.com/privacy.

APPENDIX F. VERSION HISTORY

Version	Adopted	Effective	Summary of Changes
1.0	June 1, 2026	June 1, 2026	Initial adoption. Reviewed and reaffirmed without amendment on September 19, 2026.

CERTIFICATE OF ADOPTION

The undersigned certifies that the foregoing Privacy Policy, Version 1.0, consisting of Articles 1 through 21 and Appendices A through F, was duly adopted by Saccade, Inc. on June 1, 2026, is effective as of June 1, 2026, was reviewed and reaffirmed without amendment on September 19, 2026, and is the complete and current statement of the Company's privacy practices within its scope as of the date of this certificate.

SACCADE, INC.

By: Shreyas Bhardwaj

Title: Founder and Chief Executive Officer

Date: September 19, 2026