

Helix Consumer Health Data Privacy Notice

Last updated: 22 October 2026

This is a directly accessible copy of the relevant Helix policy provisions. Read it together with the Terms of Service and Privacy Policy. Required individual choices and applicable mandatory rights remain separate.

Contents

Part 1. Consumer Health Data Privacy Notice

Part 1. Consumer Health Data Privacy Notice

1 Scope and responsible entity

Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States, processes consumer health data for HelixMatchGlobal.com and the Helix app. Contact Legal@helixmatchglobal.com to exercise rights or ask questions. This standalone notice provides additional health-data disclosures, including under Washington's My Health My Data Act where applicable. It supplements the Privacy Policy; it is not consent to collection or sharing and does not reduce protections under other laws.

2 Categories collected

Where relevant to a requested feature and lawfully provided, we process reproductive/fertility information and family-building intentions; selected diseases, carrier conditions, test statuses and report information; health/genetic comparison results; donor health/history information from lawful sources; and AI inputs or outputs/inferences that reveal or imply health, genetic or reproductive information. Associated profile, account and technical identifiers can link these categories to a person. Health-related searches, filters, likes, messages, expense discussions or attachments can reveal a person's attempt to obtain health/reproductive services, preferences or treatment-related costs. Location choices and approximate technical location may become health data when they identify or infer such activity. We do not use precise-location geofences around health facilities to identify care-seekers, track them or deliver health-related advertising. This notice does not authorise collecting unneeded information or any future biological sample, biometric template or model-training dataset.

3 Sources

We receive data from the individual and the features they request; another user only where that submission is authorised and lawful; separately authorised laboratory/provider integrations if offered; and donor banks or other external sources only where an appropriate lawful basis and necessary rights exist. We generate comparisons and illustrative inferences from authorised inputs. Public availability alone is not permission for sensitive-data reuse. Technical records arise from operating and protecting the service.

4 Purposes

We use only necessary and lawfully authorised information to provide selected sensitive-profile/discovery functions, carrier comparison, requested Future Family calculations/illustrations, intended communications and expense discussions; deliver support; secure the service and investigate abuse; process valid privacy requests; meet legal requirements; and establish or defend lawful claims where permitted. Sensitive-data conditions apply separately to safety or legal handling where required. General training of the image model on personal inputs is not a current purpose. Any future training proposal requires separate disclosures and any required optional consent in advance. Health/genetic data and private content are not used for advertising or sold under this notice.

5 Categories shared and recipients

Other members receive only the selected profile/health fields, status or comparison results, messages/expense attachments and AI outputs that the relevant permission and feature disclose. Report documents are not public by default. A match does not grant all-data access. A user's own consent cannot authorise another person's data without their lawful permission.

Processors receive only what is needed for hosting, authorised support/security, delivery and other requested operational functions under applicable contracts. Amazon Web Services is the confirmed hosting provider. Google Firebase Analytics receives technical usage information under the Privacy Policy, but genetic reports, condition choices, private messages, photos, AI prompts/traits and reproductive expense documents must not

be included as analytics payloads. Health-related usage and identifiers must be assessed to prevent inadvertent health disclosure. An independent laboratory, clinic or donor bank receives health data from Helix only where you expressly request and lawfully authorise the relevant transfer or another applicable legal requirement permits it. Listing an institution does not mean records are automatically transmitted to it. Competent authorities, courts and professional advisers receive only information lawfully necessary for the relevant process, safety response or legal claim. A successor or transaction counterparty is subject to applicable health-data purpose, confidentiality and consent restrictions; financing is not permission for unrestricted health-data access. Helix does not routinely share consumer health data with affiliates under this notice. If a specific affiliate is to receive it, Helix must name it and obtain the required permissions before sharing. Categories of independent recipients include the selected other members, separately authorised healthcare providers/donor banks, lawful authorities and advisers; processor categories are described above. We do not sell consumer health data. No sale authorisation is sought as part of registration.

6 Consent and withdrawal

Where applicable, we obtain consent before collecting health data for a specified purpose and separate consent before sharing it, except to the extent a statutory requested-service or other lawful exception actually applies. The request identifies the categories, purpose, recipient categories and withdrawal method. General acceptance, a broad licence or agreement to a Privacy Policy does not replace the required permission. We do not infer a health-sharing permission from Premium payment. You can withdraw future consent through relevant controls or Legal@helixmatchglobal.com. We stop the affected consent-based activity and delete/restrict data as required. A selected feature may no longer work without necessary data, but unrelated access is not conditioned on unnecessary permission. Withdrawal does not validate past unlawful processing or invalidate earlier lawful use.

7 Access deletion and appeals

Where the applicable law provides them, you may confirm whether we collect/share/sell health data; access it and obtain the legally required list of recipients and contact information; withdraw consent; and request deletion. We verify requests proportionately, accept authorised representatives as law permits and provide accessible requests without unlawful discrimination. For Washington rights, we respond without undue delay and within 45 days, with a lawful extension of up to 45 additional days where necessary and timely notice. We delete applicable records and notify relevant processors, contractors, affiliates and other recipients as the law requires. For qualifying archived/backup systems, any statutory delay is used only as allowed, with the required isolation and outer deadline; Washington permits certain backup delay up to six months. The ordinary 30-day account restoration option does not override these rights. If we deny a request, we explain the basis and how to appeal. Email Legal@helixmatchglobal.com with the request and reason for appeal. For Washington appeals, we respond within 45 days with the result and reasons and, if denied, provide an online mechanism or other method to contact the Washington Attorney General at <https://www.atg.wa.gov/file-complaint>. Different applicable laws may require a shorter deadline or additional rights, which prevail.

8 Retention and protection

Health data is retained only for the selected purpose and a valid legal retention basis, with restricted access and appropriate safeguards. We do not keep full reports merely because it might be useful later or claim anonymity when re-identification remains possible. Account closure, consent withdrawal and processor deletion follow the Privacy Policy and stricter applicable rules. Helix does not promise absolute security or waive breach notification/remediation duties.

9 Changes and contact

Before new health categories, purposes or recipients are introduced, we update disclosures and obtain any required affirmative permission. Future payment facilitation, hosting regions or AI training are not authorised by this notice. Contact Legal@helixmatchglobal.com or Helix Match Global Inc., 254 Chapman Rd., Ste 209, Newark, DE 19702, United States.

10 Further health categories and regional rights

Consumer health data can also include mental-health disclosures, counselling, treatment and procedure histories, medications, bodily measurements, reproductive or sexual health, gender-affirming care, genetic characteristics, attempts to obtain care, accessibility requests that reveal a condition, and health information in safety reports. Helix does not collect every category as a mandatory field; information may be provided through optional content or necessary support. Identifiers and inferences can link it to you. Do not submit another person's records without authority. No biometric identification or precise-location healthcare tracking is authorised by this notice.

This notice also applies to Nevada consumer health data where its law covers the processing. Applicable rights include confirmation, access, required recipient information, withdrawal, deletion, appeals and non-discrimination, with the timing and exceptions required by that law. Contact Legal@helixmatchglobal.com for the initial request and for an appeal identified as Health Privacy Appeal. We explain a denial, any lawful extension and the relevant regulator route. Washington's specific rights and 45-day periods above remain. We do not geofence a healthcare facility to identify or track care-seekers or send health-related advertising, sell consumer health data, or obtain a sale authorisation through general acceptance.

For an authorised health-data sharing choice, the collection purpose, data categories, intended recipient categories and withdrawal route must be disclosed separately from general dating acceptance. Corporate ownership changes, source-bank publication and another member's consent do not waive these protections. The California notice and other applicable privacy rights remain additional. Required notices of a health-data security incident are not waived by the no-medical-advice disclaimer.

11 Health information in accessibility and safety communications

Health data may arise from non-prescription treatment discussions, accessibility assistance, a safety complaint or an inference about seeking care even if no medical field is completed. The purposes and protections in this notice apply to such information. Necessary safety warnings to affected people must be limited and lawfully justified; the existence of a report does not permit public disclosure of a person's diagnosis, genetic report or reporter identity. A sensitive datum is not excluded from this notice merely because it came through chat, a support form or an external source.

12 Inferred health information and non-members

Health-related inferences and identifiers remain protected where the applicable law covers them even if an inference is wrong or the affected person has never joined Helix. A rights request may identify the listing, message or generation involved without creating an account. No generated appearance is proof of a diagnosis, reproductive capacity, genetic relationship or treatment outcome. Necessary identity checks must be proportionate; a request to correct or remove such an inference does not require a full medical record. The collection, sharing, withdrawal and deletion requirements above continue to apply to these records.