MedPassport Lab Privacy Policy

Effective Date: June 17th, 2026
Last Updated: June 16th, 2026

Product Name: MedPassport Lab
Privacy Contact Email: team@medpassportlab.com
Supported Country / Region at Launch: United States
Data Hosting Provider: Supabase
File Storage Provider: Supabase Storage
Authentication Provider: Supabase Authentication
Social Login Providers: Not currently applicable
Payment Processor: Stripe
AI / Document Processing Providers: Gemini API
Analytics Providers: Vercel Analytics & PostHog Analytics
Error Monitoring Providers: PostHog

---

1. Introduction

MedPassport Lab ("MedPassport Lab," "we," "us," or "our") provides a direct-to-consumer health organization and visualization platform that helps users upload, organize, structure, view, track, and export their own lab history and related health information.

We understand that health information is highly personal and sensitive. This Privacy Policy explains what information we collect, how we use it, how we protect it, when we may disclose it, how long we retain it, and what choices and rights you may have.

This Privacy Policy is intended to be transparent and protective. However, it is not a substitute for legal compliance, security engineering, or operational discipline. Our actual product design, backend architecture, vendor agreements, deletion workflows, logging practices, and data-sharing practices must match this Privacy Policy.

By accessing or using MedPassport Lab, you agree to this Privacy Policy. If you do not agree, do not use the Service.

---

2. Important Summary

MedPassport Lab is designed as a consumer-controlled health organization tool.

We do **not** sell your personal health information.

We do **not** use your lab results, biomarker values, uploaded lab reports, or medical profile information for targeted advertising.

We do **not** provide medical advice, diagnosis, treatment, emergency services, or clinical decision-making.

We do **not** intentionally store health data in authentication-provider metadata.

We aim to minimize the amount of personal information we collect and retain.

We provide users with tools to access, export, correct, and delete their information.

We use service providers only as needed to operate, secure, maintain, and improve the Service, and we seek to use appropriate contractual protections where applicable.

This summary is provided for convenience. The full Privacy Policy below controls.

---

3. Scope of This Privacy Policy

This Privacy Policy applies to MedPassport Lab websites, applications, dashboards, upload tools, parsing tools, charting tools, export tools, account features, and related services that link to or reference this Privacy Policy.

For purposes of this Privacy Policy, the “Service” means the MedPassport Lab website, app, software, dashboard, upload features, parsing features, charting features, export features, account features, and related services.

This Privacy Policy does not apply to:

- Third-party websites, apps, or services that we do not control.
- Doctors, clinics, hospitals, laboratories, pharmacies, insurers, employer health plans, or other healthcare organizations.
- Third-party patient portals or lab portals you access outside MedPassport Lab.
- Information you independently export, download, print, email, or share outside MedPassport Lab.
- Information collected by third parties under their own privacy policies.

---

4. MedPassport Lab Is Not a Healthcare Provider

MedPassport Lab is not a doctor, clinic, hospital, laboratory, pharmacy, insurer, health plan, emergency medical service, or healthcare provider.

MedPassport Lab does not provide medical advice, diagnosis, treatment, clinical decision-making, medical testing, prescriptions, emergency care, provider-patient services, or professional healthcare services.

The Service is intended only to help users organize, visualize, and export information they choose to provide.

If you have medical questions, symptoms, abnormal lab results, medication concerns, or health concerns, contact a licensed healthcare professional.

If you are experiencing a medical emergency, call emergency services immediately.

---

5. HIPAA, Direct-to-Consumer Use, and Future B2B Use

MedPassport Lab currently operates as a direct-to-consumer product. Users choose whether to upload or enter their own information.

Depending on how the Service is used, MedPassport Lab may not be a “covered entity” or “business associate” under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, commonly known as HIPAA.

However, even when HIPAA does not apply, other privacy, consumer protection, data security, breach notification, consumer health data, unfair or deceptive practices, and state privacy laws may apply.

We treat user health information as sensitive information regardless of whether HIPAA applies.

The current Service is not intended to be offered by or on behalf of a doctor, clinic, hospital, laboratory, insurer, employer health plan, or other HIPAA-regulated entity.

If MedPassport Lab later works with healthcare providers, laboratories, insurers, employer health plans, or other regulated entities, our legal status may change. In that case, we may need to update this Privacy Policy, implement additional compliance procedures, enter into Business Associate Agreements where required, modify our security program, and change how certain information is collected, used, stored, disclosed, and retained.

Users should not assume that this direct-to-consumer Privacy Policy will apply unchanged to any future provider-facing, clinic-facing, employer-facing, insurer-facing, laboratory-facing, or B2B version of the Service.

---

6. Information We Collect

We collect information in several ways: information you provide directly, information generated through your use of the Service, information produced through document processing, and limited technical information necessary to operate and secure the Service.

6.1 Account and Authentication Information

When you create or manage an account, we may collect:

- Email address
- Authentication identifier
- Login method
- Session information
- Password reset information
- Multi-factor authentication status, if enabled
- Account creation date
- Account status
- Security and login activity
- Device and session identifiers used for security

Authentication is currently handled by Supabase Authentication.

Authentication systems are used only for login, security, and account management.

We do not intentionally store lab results, biomarkers, medical profile information, medical notes, medications, allergies, conditions, uploaded lab reports, extracted lab data, or other health information in authentication-provider metadata.

If we later add additional authentication options, such as Google login, Apple login, Microsoft/Azure login, or other social login providers, we may update this Privacy Policy as appropriate.

6.2 Health Information You Choose to Provide

You may choose to upload, enter, store, or manage health-related information, including:

- Lab reports
- Bloodwork results
- Biomarker names
- Biomarker values
- Units of measurement
- Reference ranges
- Lab names
- Report dates
- Collection dates
- Ordering provider names, if included in uploaded documents
- Medical notes
- Medications
- Allergies
- Conditions
- Procedures or surgeries
- Vaccinations
- Provider names
- Emergency contact information
- Basic medical profile information
- Health-related notes
- Other health-related records you choose to provide

You decide what information to provide. You should not upload or enter information unless you are comfortable storing and processing it through the Service.

6.3 Uploaded Files and Documents

If you upload lab reports or other health documents, those files may contain sensitive personal information, including your name, date of birth, provider names, lab names, test results, account numbers, addresses, insurance-related information, medical record numbers, or other identifiers.

Depending on product settings and available features, we may:

- Temporarily process uploaded files.
- Store uploaded files in private storage.
- Extract structured data from uploaded files.
- Allow you to delete uploaded files.
- Allow you to choose whether original files remain stored after extraction.
- Retain only structured lab data after extraction if the original file is deleted.

If the Service provides a “delete original file” or similar feature, our intent is to remove the original uploaded file from active user-accessible storage after the deletion request is processed, unless retention is required for legal, security, fraud prevention, abuse prevention, dispute resolution, or operational reasons.

Users should understand that deleting an original uploaded file may not delete structured lab values that were extracted from that file unless the user also deletes those extracted records or requests account deletion.

6.4 Extracted Lab Data

When you upload a lab report, the Service may attempt to extract structured information, including:

- Test names
- Biomarker names
- Biomarker values
- Units
- Reference ranges
- Result flags
- Collection date
- Report date
- Lab source
- Notes appearing on the report
- Confidence scores
- Parsing status
- Original marker names
- Normalized marker names

Automated extraction can be incorrect. You are responsible for reviewing extracted information before saving, relying on, exporting, or sharing it.

6.5 Manually Entered Information

You may manually enter information into the Service, including lab values, notes, medications, allergies, conditions, procedures, provider names, or other health profile information.

Manual entries are stored so that you can view, edit, track, and export them.

6.6 Usage and Technical Information

We may collect limited usage and technical information necessary to operate, secure, maintain, debug, and improve the Service, such as:

- IP address
- Device type
- Browser type
- Operating system
- App version
- Feature usage
- Upload status
- Error events
- Log timestamps
- Security events
- Approximate location inferred from IP address
- Referral source
- Performance information
- API request metadata
- Crash or error diagnostics
- Fraud and abuse signals

We do not intentionally include lab values, medical notes, uploaded reports, extracted health information, medications, diagnoses, conditions, or detailed health information in analytics events, advertising tools, support tools, crash reports, or error logs.

If diagnostic logs or error reports accidentally contain health information, we will treat that information as sensitive and handle it according to this Privacy Policy and applicable law.

If we later add product analytics providers, error monitoring providers, or similar technical tools, we may update this Privacy Policy as appropriate.

6.7 Payment Information

If we offer paid features, subscription plans, early-access plans, or paid exports, payments may be processed by a third-party payment provider such as Stripe.

We do not store full payment card numbers on our servers.

Payment processors may collect billing details, transaction identifiers, payment method details, subscription status, and related payment information according to their own terms and privacy policies.

If paid features are not currently enabled, this section applies only if and when we introduce paid features.

6.8 Communications, Support, Surveys, and Feedback

If you contact us, join a waitlist, respond to a survey, request support, provide feedback, or participate in user research, we may collect:

- Name
- Email address
- Message content
- Survey responses
- Feedback
- Support request details
- Product experience information
- Screenshots or attachments you choose to provide

Do not send sensitive health information through ordinary email or unsecured support channels unless we specifically provide a secure method for doing so.

---

7. How We Use Information

We use information to provide, operate, secure, improve, maintain, and support MedPassport Lab.

Specifically, we may use information to:

- Create and manage accounts
- Authenticate users
- Maintain secure sessions
- Process uploaded files
- Extract structured lab data
- Allow users to review and edit extracted information
- Store confirmed lab results
- Generate biomarker timelines
- Display charts and trends
- Maintain user medical profile sections
- Generate exports
- Provide customer support
- Debug technical issues

- Detect and prevent unauthorized access
- Monitor abuse, fraud, and misuse
- Improve parser quality
- Improve product functionality
- Communicate service updates
- Process payments, if paid features are enabled
- Enforce our Terms of Service
- Comply with legal obligations
- Maintain audit and security logs
- Protect the rights, privacy, safety, and security of users and MedPassport Lab

We may use aggregated, de-identified, or statistical information to understand product performance and usage patterns, provided that such information does not reasonably identify you.

---

8. Lab Report Parsing, AI, and Automated Processing

The Service may use software, rules-based extraction, optical character recognition, machine learning, artificial intelligence, large language models, or other automated tools to process uploaded documents and extract structured information.

Automated processing may be inaccurate, incomplete, delayed, or unavailable.

You understand that:

- A lab value may be extracted incorrectly.
- A unit may be misread.
- A reference range may be omitted or incorrect.
- A biomarker may be mapped to the wrong standardized name.
- A report date or collection date may be misidentified.
- Charts and trends may be wrong if source data is wrong.
- Duplicate results may occur.
- Some results may be missed entirely.

MedPassport Lab may display confidence indicators or review prompts, but these do not guarantee accuracy.

Unless we provide notice and obtain any required consent, we do not use identifiable user health information to train third-party foundation models.

If third-party AI, OCR, parsing, or document processing providers are used, they must be authorized by us to process information only as needed to provide services to MedPassport Lab, and we will seek appropriate contractual protections, such as Data Processing

Agreements, confidentiality obligations, deletion obligations, restrictions on model training, and restrictions on independent use of user data.

Users should review extracted information before saving, relying on, exporting, or sharing it.

---

9. Consumer Health Data Notice

Certain laws may define some of the information we collect as “consumer health data,” “health data,” “sensitive personal information,” “sensitive data,” or similar terms.

Consumer health data may include information that identifies or can reasonably be linked to a person and relates to that person’s past, present, or future physical or mental health status.

MedPassport Lab may collect consumer health data that you choose to provide, including:

- Lab reports
- Biomarker values
- Medical profile information
- Medications
- Allergies
- Conditions
- Procedures
- Health notes
- Provider names
- Health-related files
- Health-related inferences created from your information
- Other health information you enter

We collect and use consumer health data to:

- Provide the Service you request
- Organize your records
- Display lab timelines
- Generate charts
- Generate exports
- Maintain your account
- Secure the Service
- Provide support
- Improve product functionality
- Comply with law
- Prevent fraud, abuse, and unauthorized access

We do not sell consumer health data.

We do not use consumer health data for targeted advertising.

We do not use consumer health data to determine eligibility for employment, credit, insurance, housing, or similar decisions.

We do not share consumer health data except as described in this Privacy Policy, including with service providers or processors, at your direction, for legal/security reasons, or in connection with a business transfer subject to appropriate safeguards and applicable law.

Where applicable law requires specific consent before collecting, using, or sharing consumer health data, we will seek to obtain that consent.

You may request access, correction, deletion, or export of your information by using in-app tools or contacting us at team@medpassportlab.com.

---

10. Service Providers, Processors, and Vendor Controls

We may use third-party service providers, processors, contractors, or vendors to help us operate, secure, maintain, and improve the Service.

These providers may include:

- Cloud hosting providers
- Database infrastructure providers
- File storage providers
- Authentication providers
- Payment processors, if paid features are enabled
- Email delivery providers
- Security monitoring providers
- Error monitoring providers, if enabled
- Customer support providers
- Document processing providers, if enabled
- AI, OCR, or parsing providers, if enabled
- Analytics providers limited to non-health operational data, if enabled
- Product infrastructure providers

Where appropriate, we seek to classify these providers as service providers, processors, contractors, or equivalent restricted vendors under applicable law, rather than independent third parties that may use user information for their own purposes.

Where appropriate, we require contractual protections, which may include:

- Data Processing Agreements

- Confidentiality obligations
- Security obligations
- Restrictions on selling data
- Restrictions on targeted advertising
- Restrictions on using data for model training
- Restrictions on independent use of user data
- Deletion or return obligations
- Subprocessor disclosure or approval requirements
- Breach or security incident notification obligations
- Assistance with user rights requests

We do not authorize service providers to use identifiable consumer health data for their own advertising, profiling, model training, resale, or unrelated commercial purposes.

Before using a new vendor that may process consumer health data, we intend to review whether that vendor is appropriate for sensitive health information and whether contractual restrictions are needed.

---

11. How We Share Information

We may disclose information only in limited circumstances.

11.1 Service Providers and Processors

We may share information with service providers and processors that help us provide the Service.

These providers may process information only as needed to perform services for us and must not use information for their own purposes except as permitted by contract or law.

11.2 At Your Direction

You may choose to export, download, print, email, or share your information with doctors, healthcare providers, family members, caregivers, emergency contacts, or others.

You are responsible for deciding what to share and with whom.

Once information is exported, downloaded, printed, emailed, or shared outside MedPassport Lab, we may not be able to control how the recipient uses, stores, or rediscloses it.

11.3 Legal, Safety, and Security Disclosures

We may disclose information if we believe disclosure is reasonably necessary to:

- Comply with applicable law
- Respond to legal process
- Enforce our Terms of Service
- Protect user safety
- Investigate security incidents
- Prevent fraud or abuse
- Protect the rights or property of MedPassport Lab
- Detect or prevent unauthorized access
- Comply with regulatory obligations
- Defend legal claims

11.4 Business Transfers

If MedPassport Lab is involved in a merger, acquisition, financing, reorganization, bankruptcy, sale of assets, or similar transaction, user information may be transferred as part of that transaction.

If such a transfer occurs, we will take reasonable steps to require that transferred information remains subject to privacy protections consistent with this Privacy Policy, unless users are provided notice and any required choice or consent.

11.5 Aggregated or De-Identified Information

We may use and disclose aggregated or de-identified information that does not reasonably identify a specific user.

We will not attempt to re-identify de-identified information except to test de-identification methods, comply with law, investigate security issues, or as otherwise permitted by law.

---

12. Advertising, Analytics, and Tracking

MedPassport Lab does not use lab results, biomarker values, medical profile information, uploaded health documents, health notes, or consumer health data for targeted advertising.

We do not sell personal health data to advertisers.

We do not intentionally disclose personal health data to advertising networks.

We do not place third-party advertising pixels or retargeting technologies on pages where users upload, view, manage, chart, or export health records unless we update our practices, provide notice, and obtain any legally required consent.

If MedPassport Lab displays ads or sponsorships in the future, we will aim to use privacy-protective formats such as:

- Non-personalized sponsorships
- Contextual placements not based on user health data
- Directly served banners without third-party behavioral tracking
- No health-data-based ad targeting
- No sharing of lab values or medical profile information with ad networks

We may use limited product analytics to understand app performance, but analytics must not include raw lab values, uploaded files, medical notes, diagnoses, medications, or other sensitive health details.

Marketing and advertising tools may be used on public landing pages where users have not uploaded, viewed, or entered health data. We do not intend to use those tools inside authenticated health-data pages unless we update our practices and obtain any legally required consent.

---

13. Data Security

We use reasonable administrative, technical, and organizational safeguards designed to protect user information.

These safeguards may include:

- Authentication controls
- Session controls
- Database access restrictions
- Row-level security policies
- Private file storage

- Encryption in transit
- Access logging
- Least-privilege access controls
- Separation of authentication data and health data
- Restricted service-role access
- Data minimization
- Secure development practices
- Security monitoring
- Account deletion workflows
- Export controls
- Vendor review procedures
- Environment variable protections
- Restricted production database access
- Access reviews
- Incident response procedures

No security system is perfect. We cannot guarantee that unauthorized access, loss, misuse, disclosure, alteration, or destruction of information will never occur.

You are responsible for maintaining the confidentiality of your login credentials and for using a secure device and network.

---

14. Data Retention

We retain personal information for as long as reasonably necessary to provide the Service, maintain your account, comply with legal obligations, resolve disputes, prevent fraud or abuse, enforce our agreements, and protect the Service.

Health information may be retained until:

- You delete specific records.
- You delete your account.
- We no longer need the information to provide the Service.
- Retention is no longer legally or operationally necessary.

If you delete your account, we will delete or de-identify personal information associated with your account unless retention is required for legal, security, fraud prevention, dispute resolution, or legitimate business purposes.

Some limited records may be retained where necessary for:

- Security logs
- Fraud prevention

- Payment records, if paid features are enabled
- Tax or accounting obligations, if applicable
- Legal compliance
- Dispute resolution
- Enforcement of our agreements
- Evidence of consent or deletion requests

Where we retain such records, we will seek to limit them to what is reasonably necessary.

---

15. Account Deletion and Data Export

MedPassport Lab will provide users with reasonable tools to export and delete their information.

You may be able to:

- Delete individual lab results
- Delete manually entered information
- Delete uploaded files, if file deletion is supported
- Export your lab history
- Export your medical profile
- Request account deletion

Before deleting your account, you should export any information you want to keep. Once deletion is completed, we may not be able to recover your data.

Account deletion is intended to remove or de-identify personal information associated with your account from active systems, subject to legal obligations, security needs, dispute resolution needs, and other limitations described in this Privacy Policy.

Deleting your account from the authentication provider may not automatically delete all app data unless our systems are configured to perform linked deletion. Our intended account deletion workflow is to delete or de-identify app data stored in Supabase and related active systems when an account deletion request is completed.

---

16. Your Privacy Choices and Rights

Depending on your location and applicable law, you may have rights to:

- Access your information
- Correct inaccurate information
- Delete information

- Export information
- Withdraw consent
- Restrict certain processing
- Object to certain processing
- Appeal a denied privacy request
- Obtain information about data sharing
- Opt out of certain data uses where applicable
- Limit certain uses of sensitive information where applicable

You may exercise available rights through in-app settings or by contacting us at team@medpassportlab.com.

We may need to verify your identity before fulfilling certain requests.

We will respond to privacy requests within the time required by applicable law.

If we deny a request, in whole or in part, we will provide an explanation when required by law and will provide appeal rights where applicable.

---

17. State Consumer Health Data and Privacy Rights

Certain U.S. state privacy laws may give residents specific rights regarding personal information, sensitive personal information, or consumer health data.

These laws may include consumer health data laws or privacy laws in states such as Washington, Nevada, Connecticut, California, and other jurisdictions that may adopt similar rules.

Depending on where you live and whether a law applies to MedPassport Lab, you may have rights to access, delete, correct, export, withdraw consent, appeal, or limit certain uses or disclosures of your information.

Some state consumer health data laws define “sharing” broadly. For that reason, MedPassport Lab treats disclosures to vendors, AI tools, document processors, analytics providers, storage providers, and error monitoring providers as sensitive from a compliance perspective.

Where required, we will seek to structure vendor relationships through appropriate service provider, processor, contractor, or similar agreements so vendors are restricted from using consumer health data for their own independent purposes.

If a state consumer health data law requires specific consent before collection, use, or sharing, we will seek to obtain that consent.

To submit a request, contact us at team@medpassportlab.com.

---

18. Data Breach and Security Incident Notification

If we discover a security incident involving personal information, consumer health data, or other protected information, we will investigate and respond as appropriate.

Where required by law, we will notify affected users, regulators, consumer reporting agencies, attorneys general, the Federal Trade Commission, media outlets, or other parties.

Notification timing and content may depend on the nature of the incident, applicable law, law enforcement needs, and our investigation.

We may take steps to contain, investigate, remediate, document, and prevent similar incidents.

---

19. Children and Minors

MedPassport Lab is intended only for users who are at least 18 years old.

We do not knowingly collect personal information from children under 13.

If we learn that we have collected personal information from a child under 13, we will take reasonable steps to delete it.

Users may not create accounts on behalf of minors unless we expressly introduce a legally reviewed family, parent, guardian, or caregiver feature.

---

20. Communications

We may send you service-related messages, including:

- Account notices
- Security alerts
- Privacy updates
- Terms updates
- Payment notices, if paid features are enabled
- Product functionality notices
- Support messages

- Data export or deletion notices

You may also receive optional marketing emails if you opt in or if permitted by law. You can unsubscribe from marketing emails, but you may still receive important service-related messages.

Do not include sensitive health information in ordinary email replies unless we provide a secure method for doing so.

---

21. International Users

MedPassport Lab is initially intended for use in the United States.

If you access the Service from outside the United States, you understand that your information may be processed in the United States or other jurisdictions where we or our service providers operate.

Other countries may have data protection laws different from those in your location.

We may restrict access from certain jurisdictions if we determine that legal, privacy, security, or operational risks are too high.

---

22. Do Not Track and Global Privacy Signals

Some browsers offer “Do Not Track” signals. Because there is no uniform standard for how such signals should be interpreted, we may not respond to them unless required by law.

Where legally required, we will seek to honor applicable opt-out preference signals, universal opt-out mechanisms, or global privacy control signals for the processing activities covered by those laws.

We do not use health data for targeted advertising.

---

23. Changes to This Privacy Policy

We may update this Privacy Policy from time to time.

If we make material changes, we will provide notice through the Service, by email, or by other appropriate means.

The updated Privacy Policy will be effective when posted unless stated otherwise.

Your continued use of the Service after the updated Privacy Policy becomes effective means you agree to the updated Policy.

If required by law, we will obtain consent before applying material changes to certain data practices.

---

24. Contact Us

If you have questions, requests, or concerns about this Privacy Policy or your information, contact us at:

MedPassport Lab
Privacy Email: team@medpassportlab.com