MedPassport Lab Data Compliance & Privacy Safeguards Overview

Last Updated: June 22nd, 2026
Product: MedPassport Lab
Website: https://medpassportlab.com
Contact: team@medpassportlab.com
Status: Early-stage MVP / web-only product

1. Purpose of This Document

This document explains MedPassport Lab's current approach to data privacy, security, responsible health-data handling, and compliance planning.

MedPassport Lab is a student-founded health-tech startup that helps users organize personal bloodwork records into a private biomarker timeline. Users can upload lab report PDFs, review extracted biomarker values before saving, view trends over time, and prepare cleaner summaries for doctor visits.

MedPassport Lab is designed as a personal health-record organization and visualization tool. It is not a medical provider, diagnostic tool, treatment tool, clinical decision-support system, emergency medical service, or substitute for a licensed healthcare professional.

Because MedPassport Lab handles sensitive personal health information, we are building the product around privacy, user control, careful data handling, and clear non-medical positioning from the beginning.

2. Product Scope and Intended Use

MedPassport Lab is intended to help users:

- Upload personal lab report PDFs;
- Review extracted biomarker values before saving them;
- Organize bloodwork history over time;
- View biomarker trends against reference ranges;
- Identify which values are inside or outside the reference ranges shown in the user's own report;
- Generate appointment-friendly summaries;
- Ask general educational questions about their stored results through a guarded AI assistant.

MedPassport Lab is not intended to:

- Diagnose medical conditions;
- Treat, cure, prevent, or manage disease;
- Recommend medications;
- Recommend supplement dosages;
- Replace doctors, registered dietitians, or licensed clinicians;
- Provide emergency advice;
- Make clinical decisions for users;
- Act as a medical device;
- Serve as a provider-facing electronic health record.

All product messaging, AI responses, exports, and user-facing explanations should reinforce that MedPassport Lab is for organization, visualization, and education only.

3. Current Legal and Compliance Posture

MedPassport Lab is currently a direct-to-consumer, user-directed product. Users choose whether to upload their own lab reports and whether to save extracted results into their account.

At this stage, MedPassport Lab is not presenting itself as a healthcare provider, health plan, healthcare clearinghouse, or clinical service. MedPassport Lab is also not currently acting on behalf of a HIPAA-covered entity.

If MedPassport Lab later works directly with a healthcare provider, nursing home, assisted living facility, clinic, employer health program, lab, insurer, or other organization that may trigger additional legal obligations, MedPassport Lab will seek legal review before launching that partnership. If required, MedPassport Lab will evaluate whether a Business Associate Agreement, data-processing agreement, consent flow, or other compliance document is needed.

MedPassport Lab recognizes that even when HIPAA does not apply, consumer health data may still be regulated by federal and state privacy, consumer protection, health-breach, and data-security laws.

4. Data We May Process

Depending on what a user chooses to provide, MedPassport Lab may process:

- Account information, such as email address and login credentials;
- Uploaded lab report PDFs;
- Extracted biomarker names, values, units, reference ranges, and collection dates;
- User-confirmed biomarker results;
- User edits or corrections;

- User-generated notes, if the feature is enabled;
- Exported report summaries;
- Basic product usage data needed to operate and improve the service;
- Support messages sent by the user;
- AI chatbot questions and responses, if the AI feature is enabled.

MedPassport Lab should avoid collecting information that is not needed for the product's core purpose.

5. Data We Should Avoid Collecting Unless Necessary

MedPassport Lab should not request or intentionally collect unnecessary sensitive information such as:

- Social Security numbers;
- Government identification numbers;
- Insurance policy numbers;
- Payment card numbers stored directly by MedPassport Lab;
- Full medical histories unrelated to uploaded lab reports;
- Family member records unless the user has authority to upload them;
- Clinical diagnoses unless already present in a user-uploaded document;
- Location tracking data;
- Advertising identifiers on health-data pages;
- Unnecessary demographic or identity information.

If any of this information appears inside an uploaded lab report, MedPassport Lab should handle it carefully, avoid exposing it unnecessarily, and consider redaction/minimization where technically feasible.

6. Core Privacy Principles

MedPassport Lab follows these privacy principles:

User Control

Users should control what they upload, review, save, export, and delete.

Review Before Save

Extracted biomarker data should not become part of the user's permanent timeline until the user has had a chance to review and confirm it.

Data Minimization

MedPassport Lab should collect only the data needed to provide the product's core functionality.

No Sale of Health Data

MedPassport Lab should not sell user health data.

No Advertising Use of Health Data

User lab results, biomarker values, uploaded reports, and health timelines should not be used for advertising targeting.

Purpose Limitation

Health data should be used only to provide, secure, support, and improve the MedPassport Lab product.

Deletion Rights

Users should be able to delete individual results, uploaded reports, and their account data where technically and legally feasible.

Plain-Language Transparency

Users should be told what happens when they upload a report, what is saved, what is not saved, and how they can delete their data.

7. Security Safeguards

MedPassport Lab's security approach should include:

- Encrypted connections using HTTPS;
- Private, per-user file storage;
- Row-level access controls so users can only access their own records;
- Authentication controls through a trusted authentication provider;
- Separation of authentication data and health-record data where feasible;
- Least-privilege access for internal tools and services;
- Restricted administrative access;
- Secure API keys and environment variables;
- No secrets stored in frontend code;
- Regular review of database permissions and storage bucket policies;
- Logging of security-relevant events without storing unnecessary health data in logs;
- Prompt revocation of exposed credentials;
- Secure deletion workflows where technically feasible;
- Basic backup, recovery, and incident-response planning once the product matures.

MedPassport Lab should not claim “bank-level security,” “HIPAA compliant,” “fully compliant,” “zero risk,” or “medical-grade security” unless those claims have been reviewed and can be substantiated.

8. Access Control

User health records should be accessible only to:

- The authenticated user who owns the account;
- Authorized systems required to provide the service;
- Limited internal personnel or operators only when necessary for support, debugging, security, or legal compliance;
- Approved subprocessors required to provide hosting, authentication, storage, AI processing, or other service infrastructure.

Internal access to user health data should be limited, logged where possible, and avoided unless needed.

9. AI Data Handling

MedPassport Lab may provide an AI chatbot feature that helps users understand their stored data in plain English.

The AI assistant should be limited to:

- Explaining biomarkers generally;
- Summarizing user-provided lab values;
- Comparing values across time;
- Explaining whether values are inside or outside the reference ranges shown in the report;
- Providing general nutrition and lifestyle education;
- Helping users prepare questions for a licensed healthcare professional.

The AI assistant should not:

- Diagnose disease;
- Treat medical conditions;
- Recommend medications;
- Recommend supplement dosages;
- Tell users to stop or start prescriptions;
- Create disease-specific treatment plans;
- Claim that a food, supplement, or behavior will fix a lab result;
- Replace a doctor, registered dietitian, or licensed clinician;
- Handle emergencies.

AI Data Minimization

When possible, MedPassport Lab should send only the minimum necessary structured data to the AI model, such as:

- Biomarker name;
- Value;
- Unit;
- Reference range;
- Date;
- Trend label;
- User question.

MedPassport Lab should avoid sending unnecessary identifiers such as full name, birthdate, address, or full uploaded PDF text unless required for the specific feature and supported by appropriate legal, privacy, and vendor safeguards.

AI Provider Review

Before sending sensitive user data to any AI provider, MedPassport Lab should review:

- Whether the AI service is paid or unpaid;
- Whether inputs or outputs may be used for training;
- Whether human reviewers may access content;
- Retention periods;
- Security controls;
- Whether a business or enterprise plan is needed;
- Whether a Business Associate Agreement is required for any future HIPAA-covered use case.

MedPassport Lab should not use unpaid AI services for sensitive personal health data unless the provider's terms clearly allow it and appropriate safeguards are in place.

10. Health Claims and Marketing Compliance

MedPassport Lab should market itself as a health-record organization, biomarker timeline, and appointment-preparation tool.

Acceptable positioning includes:

- "Organize your bloodwork in one private timeline."
- "Track biomarker trends over time."
- "Review extracted lab values before saving."
- "Prepare cleaner summaries for doctor visits."
- "Ask general educational questions about your results."

MedPassport Lab should avoid claims such as:

- “Diagnose your bloodwork.”
- “Find out what is wrong with you.”
- “Fix your lab results.”
- “Reverse disease.”
- “Avoid doctors.”
- “Detect disease early.”
- “AI doctor.”
- “Personalized treatment plan.”
- “Know exactly what to eat or take.”

Any health-related claim should be truthful, not misleading, and supported by reliable evidence.

11. User Consent and Notice

Before uploading a lab report, users should be clearly informed that:

- They are choosing to upload personal health information;
- The uploaded report may contain sensitive data;
- The app may extract biomarker values from the report;
- The user should review extracted values before saving;
- MedPassport Lab is not providing medical advice;
- The user can delete reports or results;
- The user should not upload someone else’s records unless authorized.

A short upload notice should appear near the upload flow.

Suggested upload notice:

“By uploading a report, you confirm that you have the right to upload this file. MedPassport Lab will process the report to extract biomarker information for your review. Nothing should be treated as medical advice, diagnosis, or treatment. Please review all extracted results before saving.”

12. Deletion and Account Closure

MedPassport Lab should allow users to request or perform deletion of:

- Individual biomarker results;
- Uploaded reports;
- Generated exports;
- Account data.

Deletion should be completed within a reasonable time unless retention is required for fraud prevention, legal compliance, security, billing records, or legitimate operational needs.

If backups are implemented later, MedPassport Lab should clearly explain how backup deletion works and how long backup data may persist.

If backups are not currently implemented, MedPassport Lab should not claim backup deletion or backup retention practices that do not exist.

13. Incident Response

MedPassport Lab should maintain a basic incident-response plan covering:

- Detection of unauthorized access;
- Containment of the issue;
- Credential rotation;
- Investigation of affected systems and users;
- Documentation of what happened;
- User notification where required;
- Regulator or platform notification where required;
- Post-incident fixes.

Potential incidents include:

- Unauthorized account access;
- Exposed API keys;
- Public storage bucket misconfiguration;
- Database permission errors;
- Incorrect row-level security policies;
- Accidental exposure of user records;
- Vendor breach;
- AI provider data-handling issue.

14. Vendor and Subprocessor Management

MedPassport Lab should maintain a list of vendors and subprocessors that may process user data.

Current or expected categories may include:

- Hosting provider;
- Database provider;
- File storage provider;
- Authentication provider;

- AI model provider;
- Email provider;
- Payment processor, if paid plans are enabled;
- Error monitoring provider, if enabled;
- Analytics provider, if enabled.

Before adding a vendor, MedPassport Lab should review whether that vendor will receive health data, account data, payment data, or only non-sensitive operational data.

MedPassport Lab should avoid sending health data to analytics, ad platforms, or tools that do not need it.

15. Analytics and Advertising

MedPassport Lab should not place advertising pixels or retargeting pixels on authenticated health-data pages.

Analytics, if used, should avoid collecting:

- Uploaded lab report content;
- Biomarker names tied to individuals;
- Biomarker values;
- User health timelines;
- Generated summaries;
- Chatbot health questions;
- Full URLs containing sensitive data.

Analytics should focus on product events that do not reveal health information, such as:

- Account created;
- Upload started;
- Upload completed;
- Review screen opened;
- Export clicked;
- Settings opened.

16. Children and Minors

MedPassport Lab should not knowingly collect personal health information from children under the age required by applicable law without appropriate consent.

Because the founders are minors, external legal, payment, partnership, and compliance obligations should be handled with support from an adult operator, guardian, attorney, or legally formed entity as the business matures.

17. Pilot Program Safeguards

For pilots with senior living, assisted living, nursing homes, families, or community organizations, MedPassport Lab should use a cautious pilot structure:

- Participation should be optional;
- Residents or families should decide whether to use the product;
- Staff should not be required to upload resident records;
- MedPassport Lab should not ask facilities to share resident health data directly unless legal review has occurred;
- Users should upload their own records or have an authorized family member assist;
- MedPassport Lab should provide plain-language privacy and medical-disclaimer notices;
- Feedback should be collected without exposing private health information whenever possible.

18. Compliance Roadmap

As MedPassport Lab grows, the team should work toward:

1. Finalizing privacy policy, terms of service, accessibility statement, and AI disclosure;
2. Creating a vendor/subprocessor list;
3. Completing a row-level security and private-storage review;
4. Creating a written incident-response plan;
5. Adding data export and deletion workflows;
6. Reviewing state consumer health-data obligations;
7. Reviewing HIPAA implications before any provider/facility partnership;
8. Creating AI safety and refusal rules;
9. Avoiding medical claims in marketing;
10. Seeking attorney review before paid pilots, institutional partnerships, or handling data on behalf of organizations.

19. Current Limitations

MedPassport Lab is an early-stage MVP and should not represent that it has completed enterprise compliance certifications unless those certifications have actually been obtained.

MedPassport Lab currently should not claim:

- HIPAA compliance;
- SOC 2 compliance;
- HITRUST certification;
- FDA clearance;
- Medical-device status;

- Full ADA compliance;
- Guaranteed security;
- Zero-risk privacy;
- Clinical accuracy;
- Diagnosis or treatment capability.

Instead, MedPassport Lab should state that it is privacy-conscious, user-controlled, and actively improving its safeguards as the product develops.

20. Summary

MedPassport Lab is being built to help users organize and understand their personal bloodwork history in a private, user-controlled timeline.

Our compliance approach is based on:

- Clear non-medical positioning;
- User review before saving;
- Data minimization;
- Private per-user storage;
- No sale of health data;
- No ad targeting based on health data;
- Careful AI boundaries;
- Deletion controls;
- Vendor review;
- Ongoing legal and security improvement.

MedPassport Lab is early, but we are taking the sensitivity of health data seriously from the beginning. Our goal is to build a product that is useful, calm, trustworthy, and respectful of the people who choose to store their health records with us.