DENIALTRACKER
CATCH DENIALS, KEEP REVENUE

Privacy Policy

Effective Date: 11/30/2025
Website: https://denialtrackerapp.com
Publisher: DenialTracker ("we," "us," "our")
This document will be edited and updated prior to the publishing of DenialTracker.

---

1. Introduction

DenialTracker respects your privacy and is committed to protecting the information you choose to process through our Service. This Privacy Policy explains what information we collect, how we use it, and how we ensure that no Protected Health Information ("PHI") is ever transmitted to or stored by us.

By installing or using DenialTracker (the "Service"), you agree to the practices described in this Privacy Policy.

---

2. PHI Handling & HIPAA Position

DenialTracker is intentionally designed not to store, transmit, or process PHI on our own systems. All PHI processed through DenialTracker remains fully inside the User's own Google Workspace environment, which is controlled entirely by the User.

We do NOT:

- **Store PHI on our servers.**

- **Transmit PHI to any server we operate.**
- **Access your patient information.**
- **Receive or retain copies of your 835 files.**
- **Require PHI to be transmitted to us for billing, support, or troubleshooting.**
- **Analyze, process, or log PHI in any form.**

User Responsibilities

You, the User, are solely responsible for:

- **Maintaining a valid Business Associate Agreement (BAA) with Google, if required by HIPAA.**
- **Ensuring your internal handling of PHI complies with applicable laws.**
- **Ensuring secure acquisition and transfer of 835 files from clearinghouses, RCM systems, SFTP servers, or third-party tools.**

If you choose to use external transfer methods (e.g., SFTP, Rclone, clearinghouse portals), you acknowledge that you are solely responsible for securing those systems and maintaining HIPAA compliance for those data-transfer paths.

DenialTracker cannot assume liability for improperly configured transfer tools, User-managed storage systems, or PHI exposure occurring outside Google Workspace.

---

3. Information We Collect

DenialTracker does not collect or store PHI, 835 files, or the contents of Google Drive.

However, we may collect limited non-PHI information necessary for licensing, subscription management, user authentication, analytics, and support.

3.1 User Account Information

- **Name**
- **Email address (Google account used with the add-on)**

3.2 Subscription & Billing Information (for paid plans, when Stripe is enabled)

- **Subscription status**
- **Billing history**
- **Contact information**

Payment methods and sensitive billing details are not stored by DenialTracker. All such data is stored securely by Stripe, a PCI Level 1–compliant payment processor.

3.3 Beta Tester Stripe Information

For beta testers, DenialTracker may create a minimal Stripe customer profile for authentication and feature-access purposes.
During beta testing:

- **No payment method is collected.**
- **No subscription is created.**
- **No charges occur or are pending.**
- **Stripe receives only basic identifiers (e.g., email, name).**

This minimal Stripe record exists only to support beta access and will not be converted into a paid subscription unless the User chooses to subscribe later.

3.4 Logs & Metadata (non-PHI)

We may collect general operational metadata, such as:

- **Error messages**
- **Installation events**
- **Feature usage count**
- **Runtime exceptions**

We do not log:

- **Patient names**

- **Claim IDs**
- **CPT/ICD codes**
- **Dates of service**
- **Remittance details**
- **Any health, clinical, or claim-level data**

All of that is kept within your Google Workspace.

---

4. How We Use Information

We use the limited non-PHI information we collect for:

- **License validation**
- **Subscription management**
- **Stripe beta access and authentication**
- **User support**
- **Product improvement**
- **Security monitoring**

We do not sell, share, rent, or trade User information.

We do not use PHI for analytics, training, support, or product development.

---

5. Data Storage & Security

Because DenialTracker does not collect or store PHI, we maintain no PHI repositories.

For non-PHI information (e.g., account data, subscription metadata):

- **Data is encrypted and stored securely.**

- **Access is restricted to authorized personnel.**
- **Systems are monitored for security events.**

Stripe independently manages all payment-related data in accordance with their own privacy and security policies.

---

6. Your Responsibilities

You agree that:

- **All PHI you process remains inside your own Google Workspace domain.**
- **You are responsible for maintaining a valid BAA with Google.**
- **You are responsible for securing your external acquisition and transfer of 835 files.**
- **You will not transmit PHI to DenialTracker for support or troubleshooting.**
- **If PHI is sent to us accidentally, we will delete it promptly but cannot assume liability for the User error.**

---

7. Data Retention

We retain only non-PHI information, and only as long as necessary to:

- **Provide the Service**
- **Manage subscriptions**
- **Comply with legal obligations**
- **Resolve disputes**
- **Enforce our Terms of Service**

We retain no PHI, because we never possess it.

---

8. Third-Party Services

Google Workspace

**DenialTracker operates entirely within the User's Google Workspace domain.
Google's privacy policies and any BAA between Google and the User govern how PHI is stored and protected.**

Stripe

**For paid subscribers - or beta testers requiring Stripe-based authentication - Stripe processes all billing-related data.
DenialTracker never accesses full payment details.
Stripe's Privacy Policy applies to any information collected during subscription or beta onboarding.**

No Other Third Parties

We do not share data with any other vendors, partners, advertisers, or analytics services.

---

9. Children's Privacy

**DenialTracker is not targeted toward children.
Any PHI related to minors processed through DenialTracker remains entirely in the User's Google Workspace environment and is never transmitted to us.**

---

10. Changes to This Privacy Policy

We may update this Privacy Policy as needed. Updates will be posted on our website, and continued use of the Service constitutes acceptance of the revised policy.

---

11. Contact Information

**For questions about this Privacy Policy:
Email: csnoke@denialtrackerapp.com**

By using DenialTracker, you acknowledge that you understand and agree to this Privacy Policy.