



Privacy Policy

Effective Date: 8/14/2026

Website: <https://denialtrackerapp.com>

Publisher: DenialTrackerLLC (“DenialTracker”, “we,” “us,” “our”)

1. Introduction

This Privacy Policy explains how DenialTracker LLC collects, accesses, uses, processes, discloses, and retains information in connection with the DenialTracker Google Workspace Add-on, the DenialTracker website, subscription and billing functions, support communications, and related services.

DenialTracker is intended for business and professional users in the United States.

This Privacy Policy applies to DenialTracker-controlled systems and services. It does not replace the privacy policies, security obligations, or contractual terms governing Google Workspace, Stripe, clearinghouses, electronic health record systems, revenue cycle management systems, or other independent third-party services used by a customer.

By creating or activating a DenialTracker subscription, including through Stripe or another billing interface used by DenialTracker, you acknowledge that you have received and reviewed this Privacy Policy.

2. Overview of DenialTracker’s Data Architecture

DenialTracker is designed with separate claim-processing and external business-service environments.

The DenialTracker Google Workspace Add-on processes remittance and claim information through the User’s Google Workspace environment using services such as Google Drive, Google Sheets, Gmail, and Google Apps Script.

DenialTracker separately operates external infrastructure for functions such as Google identity verification, subscription validation, Stripe billing operations, security controls, and limited operational logging.

DenialTracker's external billing infrastructure is not designed to receive the contents of 835 files, patient claim records, or other claim-level healthcare information processed by the Add-on.

This distinction is central to how DenialTracker handles User information.

3. Google User Data

DenialTracker accesses Google user data only as necessary to provide the User-facing features of the Service.

Depending on the permissions granted and features used, DenialTracker may access the following Google Workspace information.

Google Drive access may be used to locate, identify, and read qualifying 835 or related files used by DenialTracker.

Google Sheets access may be used to create, read, organize, modify, format, and maintain denial-tracking spreadsheets and related analytics or administrative information.

Gmail access may be used to send User-configured DenialTracker notifications and alerts through the User's Google account.

Google account identity information may be used to authenticate the User and determine which subscription or billing relationship applies to that User.

DenialTracker may receive a Google account email address, Google account subject identifier, and, where provided by Google, information identifying the User's Google Workspace hosted domain.

DenialTracker does not use Google Workspace claim information for advertising, advertising profiles, data brokerage, or sale of personal information.

4. Google API Limited Use

DenialTracker's access to and use of information received through Google APIs is limited to providing, securing, maintaining, and improving User-facing DenialTracker functionality consistent with the permissions granted by the User.

DenialTracker's use and transfer of information received through Google APIs is intended to comply with the Google API Services User Data Policy, including its Limited Use requirements.

Google user data is not transferred to third parties except where permitted by applicable Google API policies, such as where necessary to provide or secure the requested functionality, comply with applicable law, or where the User has clearly authorized the relevant action.

DenialTracker does not use Google Workspace data to train general-purpose artificial intelligence or machine-learning models.

5. Protected Health Information and Claim Data

DenialTracker may process claim-level information within a User's Google Workspace environment, and that information may include Protected Health Information ("PHI").

The DenialTracker Add-on may read 835 files from Google Drive, interpret information contained in those files through Google Apps Script, write information to Google Sheets, and send User-configured notifications through Gmail.

DenialTracker's external billing infrastructure is not designed to receive or store the contents of those files or the resulting claim-level patient information.

DenialTracker does not maintain an external database of User 835 files or patient claim records.

DenialTracker does not intentionally transmit claim-level data to its billing backend for subscription management, advertising, customer profiling, or general analytics.

6. User-Directed Sharing and Transmission

Although DenialTracker is designed to keep claim-processing functions within Google Workspace, Users control their own Google Workspace environment.

Users may choose to download files, export spreadsheets, share documents, configure Gmail recipients, forward alerts, connect other applications, or otherwise transmit information.

Information may therefore leave a particular Google Workspace domain because of User actions, Google Workspace configuration, or third-party integrations.

DenialTracker is not responsible for independent disclosure or transfer initiated by the User or by systems outside DenialTracker's control.

7. HIPAA and Google Workspace

Users are responsible for determining whether HIPAA applies to their organization and for configuring their Google Workspace environment accordingly.

Where required, Users are responsible for maintaining an appropriate Business Associate Agreement with Google and using Google services in a manner consistent with applicable healthcare privacy and security obligations.

DenialTracker does not represent that use of the Service alone makes a User HIPAA compliant.

Because DenialTracker's external infrastructure is not intended to receive PHI, DenialTracker does not currently offer a Business Associate Agreement to customers for the Service as presently designed.

Nothing in this Privacy Policy limits obligations that may apply directly to DenialTracker under applicable law.

8. Information DenialTracker Collects Outside Claim Processing

DenialTracker collects or processes limited non-claim information necessary to operate the business and provide the Service.

This may include Google account email address, Google account subject identifier, hosted Workspace domain information where supplied by Google, Stripe customer and subscription identifiers, subscription plan and status, billing dates, transaction status, promotional or trial status, and other billing-related information.

DenialTracker may also process limited operational and security information such as request identifiers, event types, timestamps generated by hosting or infrastructure systems, error categories, security events, and similar technical information needed to operate and protect the Service.

Hosting, networking, security, and infrastructure providers may independently process information ordinarily associated with internet requests, such as network or device information, in accordance with their own technical operations and privacy practices.

9. Authentication Information

When a User accesses protected DenialTracker billing functionality, DenialTracker may receive a short-lived Google identity token.

The token is used to verify the User's identity.

DenialTracker's backend derives limited identity information from the verified token, such as the User's Google subject identifier, verified email address, and hosted Workspace domain where available.

DenialTracker does not use the User's Google password for authentication and does not store Google account passwords.

DenialTracker is designed not to log raw Google identity tokens or authorization headers in application logs.

10. Stripe and Payment Information

DenialTracker uses Stripe to process subscription and payment functions.

When a User begins a subscription or an introductory period requiring a payment method, Stripe may collect information such as name, email address, billing information, payment method information, transaction data, and fraud-prevention information.

Stripe processes payment credentials according to Stripe's own systems and privacy practices.

DenialTracker does not receive or store complete credit card numbers or card security codes.

DenialTracker may receive or access limited billing information from Stripe, including Stripe customer identifiers, subscription identifiers, subscription status, plan information, payment status, billing dates, trial or promotional status, and information necessary to provide access to Stripe-hosted billing management features.

DenialTracker may associate a Google account identifier with a Stripe customer or subscription to ensure that billing resources correspond to the authenticated User.

11. Website Information

The DenialTracker website may collect information separately from the Google Workspace Add-on.

If a visitor submits a website contact form, DenialTracker may collect the visitor's name, work email address, and the contents of the message submitted.

Visitors should not include PHI, patient information, 835 files, claim information, or other sensitive healthcare information in website forms.

Information submitted through the website may be used to respond to inquiries, provide requested information, communicate with prospective customers, maintain business records, prevent misuse, and conduct appropriate sales or customer-support activities.

12. Website Analytics

DenialTracker uses or may use website analytics and performance tools to understand how the public website is discovered and used.

This currently includes Google Search Console.

DenialTracker may also use Google Analytics or similar analytics services.

When such services are enabled, they may process information such as pages visited, approximate traffic source, device or browser characteristics, interactions with website content, approximate geographic information derived from network data, and related usage information.

DenialTracker does not use website analytics to obtain or analyze patient claim information.

Analytics practices may change as DenialTracker's website evolves, and this Privacy Policy may be updated accordingly.

13. Cookies and Similar Technologies

The DenialTracker website may use cookies or similar technologies where necessary for website functionality, analytics, security, or performance.

Some third-party website and analytics providers may set or read cookies according to their own practices.

Users may control cookies through browser settings and, where available, website consent or preference controls.

Disabling certain cookies may affect website functionality or analytics but does not prevent claim processing within the DenialTracker Google Workspace Add-on.

14. Support Communications

If a User contacts DenialTracker for support, DenialTracker may collect the User's name, email address, organization information, correspondence, and other information voluntarily included in the request.

Users must not send PHI, 835 files, patient names, claim records, screenshots displaying PHI, or other sensitive healthcare information to DenialTracker support.

If DenialTracker receives PHI through an unintended support channel, DenialTracker may delete the information and may ask the User to resend the request after removing sensitive information.

15. Marketing Communications

DenialTracker may use contact information, including business email addresses, to send product announcements, feature updates, educational information, promotions, discounts, conference information, and similar marketing communications where permitted by applicable law.

Recipients may unsubscribe from marketing communications using an available unsubscribe mechanism or by contacting DenialTracker.

Opting out of marketing communications does not necessarily prevent DenialTracker from sending transactional, billing, account, security, legal, or service-related communications that are necessary to administer the User's relationship with DenialTracker.

16. How DenialTracker Uses Information

DenialTracker may use information under its control to operate and provide the Service, authenticate Users, validate subscriptions, process payments through Stripe, maintain billing access, respond to support requests, communicate with Users, maintain website functionality, improve product reliability, investigate errors, prevent fraud and abuse, maintain security, enforce the Terms of Service, comply with law, maintain business records, and develop or improve DenialTracker functionality.

Claim-level healthcare information processed through the Add-on is not used by DenialTracker's external billing systems for advertising or unrelated commercial profiling.

17. Information DenialTracker Does Not Sell

DenialTracker does not sell User PHI, claim information, Google Workspace claim data, or customer account information to data brokers or advertisers.

DenialTracker does not rent or trade patient claim information.

DenialTracker does not use claim-level PHI for behavioral advertising.

18. When Information May Be Disclosed

DenialTracker may disclose limited information to service providers that perform functions on DenialTracker's behalf, such as payment processing, infrastructure hosting, website hosting, security, analytics, and related business operations.

These providers may include Google, Stripe, Render, Webflow, Google Search Console, Google Analytics when enabled, and other providers added as reasonably necessary to operate DenialTracker.

DenialTracker may also disclose information where reasonably necessary to comply with law, legal process, court order, or governmental request; investigate fraud, abuse, security incidents, or violations of the Terms; protect the rights, safety, property, or security of DenialTracker, Users, or others; or complete a merger, acquisition, financing, restructuring, sale of assets, or similar corporate transaction.

DenialTracker does not disclose Google user data in a manner inconsistent with applicable Google API policies.

19. Google Workspace

Google independently provides and operates Google Workspace, Google Drive, Google Sheets, Gmail, Google Apps Script, authentication infrastructure, and related services.

Information processed through those services is also subject to the User's relationship with Google, Google Workspace configuration, organizational policies, and applicable Google terms and privacy practices.

DenialTracker does not control Google's independent processing of information.

20. Render

DenialTracker currently uses Render to host external backend infrastructure used for authentication verification, billing operations, subscription validation, security controls, and related operational functions.

DenialTracker's Render-hosted backend is not designed to receive 835 file contents or claim-level patient information.

Render may process technical information associated with hosting and network operations in accordance with its own practices.

21. Webflow

DenialTracker currently uses Webflow to host or operate portions of the public DenialTracker website.

Website visitors may therefore interact with infrastructure provided by Webflow.

Information submitted through website forms or processed as part of website operations may involve Webflow or related website infrastructure.

22. Security

DenialTracker uses administrative, technical, and organizational safeguards intended to protect information under its control.

These safeguards include authentication controls, restricted external backend functionality, encrypted network transport, server-controlled billing configuration, input validation, security-related logging, access restrictions, and measures intended to prevent sensitive claim information from entering the external billing environment.

DenialTracker's application logging is designed to avoid raw identity tokens, authorization headers, payment credentials, claim contents, and PHI.

No information system or internet transmission can be guaranteed to be completely secure. DenialTracker therefore cannot guarantee that unauthorized access, disclosure, alteration, or destruction will never occur.

23. Data Retention

DenialTracker retains different categories of information for different periods depending on the purpose for which the information is maintained.

Billing and transaction information may be retained as reasonably necessary for accounting, taxation, dispute resolution, fraud prevention, and legal obligations.

Account and subscription information may be retained while a User maintains a relationship with DenialTracker and for a reasonable period afterward.

Security and operational records may be retained for periods reasonably necessary to investigate incidents, maintain system integrity, detect abuse, and document security activity.

Support communications and website inquiries may be retained as reasonably necessary to respond to Users, maintain business records, resolve disputes, and improve support.

Marketing contact information may be retained until it is no longer reasonably needed or until a User exercises an applicable opt-out or deletion right, subject to records necessary to honor that opt-out.

DenialTracker does not maintain an external repository of User 835 files or claim-level patient records as part of its normal architecture.

24. Cancellation, Uninstallation, and Google Workspace Data

Canceling a DenialTracker subscription or uninstalling the Add-on does not automatically delete Google Sheets, 835 files, Gmail messages, or other information stored in the User's Google Workspace environment.

That information remains under the User's control and is subject to the User's Google Workspace settings and Google's services.

Users are responsible for deleting or retaining their own Workspace files and records.

DenialTracker may retain limited non-PHI billing, account, security, support, and legal records after cancellation as described in this Privacy Policy.

25. Privacy Requests

Depending on applicable law and the nature of the information DenialTracker maintains, Users may have rights to request access to, correction of, or deletion of certain personal information.

Users may also request information regarding DenialTracker's handling of their information or opt out of applicable marketing communications.

Requests may be submitted to csnoke@denialtrackerapp.com.

DenialTracker may need to verify the identity and authority of the requester before fulfilling a request.

Certain information may be retained despite a deletion request where retention is reasonably necessary or legally permitted for billing, taxation, fraud prevention, security, dispute resolution, compliance, or other legitimate purposes.

Requests concerning claim information stored in Google Drive, Google Sheets, or Gmail ordinarily must be handled through the User's own Google Workspace account because DenialTracker does not maintain an external copy of those records.

26. U.S. State Privacy Rights

DenialTracker is intended for Users in the United States.

Residents of certain states may have additional privacy rights under applicable state law, which may include rights relating to access, correction, deletion, portability, or information regarding certain disclosures.

The availability and scope of these rights depend on the applicable law and whether that law applies to DenialTracker or the particular processing activity.

DenialTracker will respond to valid privacy requests as required by applicable law.

27. Children's Privacy

DenialTracker is a business software product intended for authorized adult Users acting on behalf of healthcare practices, billing organizations, revenue cycle management organizations, and other businesses.

The Service is not directed to children under 18 and is not intended for children to create accounts or use independently.

The fact that a healthcare organization may use DenialTracker in connection with reimbursement records relating to pediatric patients does not make those patients Users of the DenialTracker Service.

28. United States Service

DenialTracker is presently offered for use by customers in the United States.

DenialTracker does not currently market the Service as a product designed for organizations subject primarily to non-U.S. privacy regimes.

A person who accesses the public website from outside the United States does so subject to applicable law and the limitations described in this Privacy Policy.

29. Business Transfers

If DenialTracker LLC is involved in a merger, acquisition, financing, reorganization, sale of assets, or similar transaction, information may be transferred as part of that transaction subject to applicable law and appropriate protections.

Any successor operating DenialTracker will remain responsible for information in accordance with applicable law and any privacy commitments that continue to apply.

30. Changes to This Privacy Policy

DenialTracker may update this Privacy Policy as its Service, technology, vendors, business practices, or legal obligations change.

The revised Policy will identify its effective date.

Material changes may also be communicated through the website, Service, email, or another reasonable method.

Continued use of the Service after an updated Privacy Policy becomes effective constitutes acknowledgment of the updated Policy to the extent permitted by law.

31. Contact Information

Questions, privacy requests, or concerns regarding this Privacy Policy may be directed to:

DenialTracker LLC

Email: csnoke@denialtrackerapp.com

Website: <https://denialtrackerapp.com>