Website & App Privacy Policy

Effective date: September 26, 2025

This Privacy Policy explains how SecurePractice.app (“we,” “our,” or “us”) collects, uses, discloses, and safeguards information when you use the Services. This policy is separate from the HIPAA Notice of Privacy Practices (NPP) that practices provide to patients.

Where a customer uploads content that contains protected health information (PHI), we process that content solely on behalf of the customer as their Business Associate under applicable agreements.

Who We Are

SecurePractice (also known as HIPAA Helper) is a software-as-a-service platform that helps healthcare practices, clinics, and similar organizations manage HIPAA compliance tasks, policies, and related documentation. Our services are provided through the websites **securepractice.app** and **securepractice.health**, as well as any related applications, tools, and content we operate.

1) Information We Collect

Account & Profile Data: name, business/practice name, role/title, address, phone, avatar, office type, display name, time zone, years in practice; credentials for sign-in (email/password); TOTP MFA secret/verification (Premium).

Customer-Uploaded Content: files uploaded via the Document Uploader (e.g., policies, logs, BAAs, incident forms, evidence). These files may contain personal information and, depending on customer use, PHI. We do not use upload contents for advertising.

Usage/Device Data: device/browser info, IP address, pages viewed; used to operate the Services.

Analytics: Google Analytics 4 (GA4) on the marketing site only; we do not send PHI to analytics.

Communications & Support: emails/SMS and our correspondence (reminders, product updates, support).

Payments: processed by Paddle. We do not store full payment card numbers; we may receive limited billing metadata (e.g., payer email, transaction IDs).

2) How We Use Information

We use information to provide, secure, and maintain the Services (including authentication and TOTP MFA for Premium); operate features such as the Document Uploader, templates, and reports; send reminders and product communications (marketing preferences can be managed

in profile settings); monitor performance, troubleshoot issues, and improve reliability; and comply with law and enforce our agreements.

We do **not** sell personal information or share it for cross-context behavioral advertising.

3) Cookies & Similar Technologies

Essential cookies are required to run the app. Non-essential cookies (e.g., analytics on the marketing site) help us understand site usage. You can adjust your browser settings to block non-essential cookies.

4) When We Disclose Information

We disclose information to service providers under contracts that limit their use to our instructions, including:

Firebase (Google): authentication, Firestore database, storage, and Cloud Functions.

Paddle: payments and subscription management.

SendGrid: email delivery.

Twilio: SMS delivery.

Google Cloud Logging and Firebase Performance Monitoring: operational telemetry (no PHI).

We may also disclose information to comply with law or legal process; to protect the rights, property, or safety of us, our customers, or others; or in connection with a corporate transaction (e.g., merger, acquisition, or asset sale). We do **not** grant vendors support-only access to customer data.

5) PHI, HIPAA, and Customer-Uploaded Content

Customers control whether uploads include PHI. Where uploads include PHI, we act as a Business Associate and process such data solely on the customer's behalf and instructions. PHI is encrypted in transit and at rest and is not sent to analytics or error trackers.

For patient rights and permitted uses/disclosures of PHI, see the practice's Notice of Privacy Practices (NPP).

6) Access Controls, Roles & Sessions

Roles (per customer):

Practice Admin / Compliance Officer: manages users and roles; may view/upload/download/edit content (including PHI as permitted); runs/exports reports; manages subscription and billing; changes org settings; accesses audit logs.

Practice User: can be granted Document Uploader access and, when granted, may view/upload/download/edit permitted content.

Additional controls include: MFA (TOTP) required for all Premium users; idle timeout of 30 minutes; maximum session age of 12 hours; audit logging of logins, role changes, uploads/downloads, and exports (retained for 2 years); and tenant isolation so users are restricted to their own practice.

7) Data Retention

Account data: active plus 24 months after last activity.

Uploaded evidence/docs: 6 months after Premium account cancellation or expiration.

Logs/analytics: active plus 24 months after last activity.

8) Security

We use administrative, technical, and physical safeguards, including TLS in transit, encryption at rest (Firestore/Storage), role-based access controls, least-privilege practices, and audit logging with periodic reviews. No method of transmission or storage is 100% secure, and customers must protect their credentials and MFA devices.

9) Children's Privacy

The Services are intended for organizations and their authorized adult users. We do not knowingly collect personal information directly from children under 13 (or under 16 where applicable). Customer-uploaded content may include information about minors when processed by authorized adult users; we handle such content solely on behalf of the customer.

10) California Notice (CPRA)

We do not sell personal information and do not share it for cross-context behavioral advertising. California residents may contact us regarding personal information as required by law.

11) Your Choices

Marketing emails: manage preferences in your profile or use the unsubscribe link in the email.

Access/Deletion requests: email us at privacy@securepractice.app.

Cookies: manage via the cookie banner on the marketing site and your browser settings.

12) International Users

We operate in the United States (Florida) and currently do not target EU/UK users.

13) Changes to This Policy

We may update this Policy from time to time. We will post the updated version with a new effective date. If changes materially affect your rights, we will provide additional notice where

required.

14) Contact Us

If you have questions about this Privacy Policy or our privacy practices, you can contact us at:

Email: privacy@securepractice.app