SafeRoom

Disposable end-to-end encrypted file-sharing for professionals — doctors, lawyers, journalists, accountants — who cannot use Gmail attachments or WeTransfer for sensitive documents. Sender controls expiry, downloads, views.

Category	Set 5 · Vertical/Creator
Customer	Solo + small-firm professionals handling confidential client documents — doctors, lawyers, accountants, journalists, therapists, financial advisors, M&A; consultants
Monetisation	$5/mo Basic · $12/mo Pro (audit logs + custom domain) · $39/mo Team (multi-seat + admin) · $99/mo Firm (compliance reporting)
Build effort	Low
Plan version	v1.0 — 2026-05

Executive Summary

SafeRoom is a focused file-sharing tool built for professionals whose work involves confidential client documents and whose existing options (Gmail attachments, WeTransfer, Dropbox) all have either security or workflow limitations. The product: end-to-end encrypted file-sharing with sender controls (expiry: file accessible only for N hours; download limit: N downloads max; view limit; access password optional; revoke at any time). Used by a doctor sending patient reports, a lawyer sending case documents, a journalist sharing source materials, a financial advisor sending client portfolios.

The wedge: existing tools fail at specific points. Gmail attachments are not encrypted (compliance risk for healthcare + legal + finance professionals), have 25MB limit, are not auditable. WeTransfer is encrypted in transit but stores files on their servers indefinitely + no sender controls. Dropbox shared links are perpetual + not auditable. SafeRoom is purpose-built for confidential ephemeral document sharing.

Pricing: $5/mo Basic, $12/mo Pro, $39/mo Team, $99/mo Firm with compliance reporting. Year-1 target: 5,500 paying subscribers generating ■3.2 crore annual revenue against ■40 lakh costs. Cash-positive month 2. Highly profitable niche; not a hyperscale market but a defensible focused-vertical SaaS.

The Problem

Professionals handling confidential client documents — doctors with patient reports, lawyers with case documents, journalists with source materials, accountants with client financials, therapists with session notes — face a recurring problem when they need to share these documents with the client (or with a third party at client's authorization). Email attachments are unencrypted + not auditable + compliance-rich. WeTransfer and Dropbox shared links work technically but lack the granular control + audit trail compliance requires.

The healthcare professional sending a patient report via Gmail attachment is potentially violating HIPAA (in US) or DPDP-Act medical-data provisions (in India). The lawyer sending an NDA-protected document via Dropbox shared link cannot prove (in event of dispute) when the recipient downloaded it + when the link was disabled. The journalist sharing source documents has no way to ensure the recipient cannot forward.

Enterprise-grade alternatives exist (Citrix ShareFile, Egnyte, Box Enterprise, Tresorit) but priced at $50-200/user/month + designed for large-team deployments. The solo + small-firm professional segment — millions of users globally — is unserved by appropriately-priced + appropriately-simple tools.

The Solution

SafeRoom's flow: user uploads file via web app or browser extension or mobile app; configures controls (expiry duration: 1 hour to 30 days; max downloads: 1 to unlimited; password optional; recipient email tracking); shares the SafeRoom link with recipient. Recipient opens link, authenticates if password set, downloads file. After expiry / max downloads / explicit revocation, link returns 'no longer available' message.

Encryption: end-to-end. Files are encrypted client-side before upload (browser-side encryption with per-file key); SafeRoom server stores only encrypted blob. Decryption happens client-side at recipient. SafeRoom team cannot read uploaded files; no third-party data sharing.

Sender controls. Expiry: configurable 1 hour to 30 days. Max downloads: 1 (single download) to unlimited. Password protection: optional, set by sender, transmitted to recipient out-of-band. Recipient-email gating: sender can require recipient to verify their email before download. Revocation: sender can revoke at any time. Audit log: who downloaded when from which IP (Pro tier).

Three structural differences from Gmail attachments / WeTransfer / Dropbox define the wedge. First, true end-to-end encryption (existing tools are at-most transport-encrypted; SafeRoom is server-can't-read encrypted). Second, granular sender controls (expiry + max downloads + revocation that competitors lack). Third, compliance-appropriate audit trail (Pro+ tier).

Market Opportunity

Addressable professional segment globally: ~12-18M solo + small-firm professionals handling confidential documents (US ~3M lawyers + 1M physicians + 1.4M accountants + ~250k therapists + ~125k financial advisors + ~50k journalists; similar segments globally). Per-user willingness-to-pay at $5-39/mo range is reasonable for professionals in confidentiality-regulated work.

At blended ARPU of $200/year, the SAM is ~$2.4-3.6 billion globally. Realistic 4-year capture: 0.1-0.3% = $2.4-10.8M annual revenue.

Adjacent expansion. Year 2: industry-specific tiers (SafeRoom for Healthcare with HIPAA-aligned compliance posture at premium pricing). Mobile app cross-sell (in-app document scanning + immediate encrypted share). Enterprise tier for larger firms wanting team-managed file-sharing infrastructure.

Target Customer

Primary persona: a 47-year-old solo lawyer in Chicago handling 30-40 active cases, frequently sending NDA-protected documents to clients + opposing counsel. Currently uses Dropbox shared links + worries about uncontrolled forwarding. Will pay $12/mo Pro tier for audit logs + sender controls.

Secondary persona: a 39-year-old psychiatrist in Bengaluru sending detailed clinical notes to referring physicians + patient family with patient consent. Currently uses Gmail attachments + suspects this is not HIPAA / DPDP-compliant. Will pay $5/mo Basic tier (■399/mo in India).

Tertiary persona: a 41-year-old founding partner of a 7-attorney boutique law firm in NYC needing firm-wide file-sharing with compliance reporting. Will pay $99/mo Firm tier (covers 7 attorneys + compliance reporting + admin dashboard).

Product

File upload: web app drag-and-drop, browser extension for one-click share from any web context, mobile app for on-the-go sharing.

Encryption: client-side AES-256 encryption with per-file key. SafeRoom server stores only encrypted blob.

Sender controls: expiry duration (1h to 30 days), max download count (1 to unlimited), password protection (optional, sender sets), recipient-email verification (optional), explicit revocation.

Recipient experience: click link → enter password if set → verify email if required → download file. After expiry / max downloads / revocation: 'no longer available'.

Audit log (Pro+): per-link history of who downloaded when from which IP, with exportable audit-trail reports.

Custom domain (Pro+): files shared from professional's own domain (files.lawfirm.com instead of saferoom.io/abc123) for brand professionalism.

Team workspace (Team tier): shared file management across team, role permissions, team-wide controls.

Firm compliance reporting (Firm tier): aggregated compliance reports for firm-wide file-sharing activity, HIPAA / GDPR / DPDP compliance attestation support.

Technical Architecture

Frontend: Next.js + Tailwind. Browser extension via TypeScript + manifest v3. Mobile app via React Native.

Backend: Go on Hetzner cloud (extremely lightweight — primarily blob storage + access control + audit logging).

Storage: Cloudflare R2 for encrypted blob storage (egress-free is meaningful at scale).

Encryption: client-side WebCrypto API for in-browser encryption + decryption; native iOS / Android crypto for mobile.

Authentication: SafeRoom user auth via Clerk; recipient email verification via Resend.

Audit infrastructure: structured Postgres-stored audit logs with tamper-evident hashing.

Compliance: SOC2 from year-1 (table-stakes for professional segment), HIPAA-aligned controls + BAA availability for healthcare segment, GDPR + DPDP compliance.

Business Model & Unit Economics

Four tiers. Basic ($5/mo): 50 file shares/month, basic controls (expiry + max downloads), single user. Pro ($12/mo): 500 file shares/month, audit logs, custom domain, password protection. Team ($39/mo): 5 seats, team workspace, admin controls. Firm ($99/mo): 15 seats, compliance reporting, HIPAA BAA, dedicated support.

Conversion economics: 14-day free trial converts at 16% (consumer-SaaS typical for utility tools). Distribution: 50% Basic, 30% Pro, 15% Team, 5% Firm. Monthly churn target under 4% Basic; under 2% Pro+.

Gross margin: 92% blended. Major cost: storage (~$0.40/user/month at average usage with R2 egress-free pricing), infrastructure (~$0.30/user/month).

Customer LTV: $60 × 22-month avg (Basic); $144 × 28 mo (Pro); $468 × 34 mo (Team); $1,188 × 40 mo (Firm).

Unit Economics (Year-1 base case)

Year-1 paying subscribers (target)	5,500
Blended ARPU	$60/year (~$240/year mix-weighted)
Year-1 revenue	$385,000 (~■3.2 crore)
Gross margin	92%
Customer acquisition cost (CAC)	$22
Payback period	2.7 months
Year-1 all-in costs	~■40 lakh
Year-1 net contribution	~■2.5 crore

Go-to-Market

Channel 1 — Professional-association partnerships (35%): partnerships with state bar associations + medical associations + AICPA + journalism unions for member discounts + content placement.

Channel 2 — Privacy + compliance content (30%): substantive content on professional confidentiality + HIPAA compliance + attorney-client privilege + data-protection compliance.

Channel 3 — Browser extension viral mechanics (20%): users discover SafeRoom via colleagues + clients receiving SafeRoom links + adopting themselves.

Channel 4 — Paid acquisition (15%): Google Ads on commercial-intent queries ('HIPAA-compliant file sharing', 'attorney-client document share', 'encrypted file transfer').

Roadmap (first 12 months)

- Month 1-2: MVP — web app with file upload + sender controls + end-to-end encryption + Basic tier. 400 paying subscribers.
- Month 3-4: Browser extension + audit logs + Pro tier, 1,400 paying subscribers, ■4 lakh MRR.
- Month 5-7: Team tier + workspace + admin controls, mobile apps (iOS + Android), 3,000 paying subscribers, ■10 lakh MRR.
- Month 8-10: Firm tier with compliance reporting + HIPAA BAA + custom domain, 4,500 paying subscribers.

- Month 11-12: 5,500 paying subscribers, ■3.2 crore annualised revenue.

Key Risks

- Citrix ShareFile / Egnyte / Tresorit launching SMB-priced tiers — possible. Mitigated by focus + simplicity vs. their feature breadth + India-pricing for international segments.
- Trust signals: professional segment requires verifiable security; without strong signals, conversion fails. Mitigated by SOC2 + HIPAA + open security documentation + bug-bounty program.
- Encryption misuse risk: bad actors use encrypted file-sharing for illegal content. Mitigated by clear terms-of-service + abuse-reporting mechanisms + cooperation with legitimate law enforcement (within scope of E2EE limits).
- Cloudflare R2 dependency: storage cost economics depend on R2's egress-free pricing. Mitigated by ability to migrate to S3 + alternate providers at higher cost if needed.
- Apple / Google policy changes affecting browser extension / mobile app distribution — periodic platform policy churn. Mitigated by careful compliance posture + multiple distribution channels.