

SAMPLE REPORT

AI Vendor Risk Assessment

Prepared for Meridian Pediatric Therapy Group (fictional client) - 42 employees, 3 locations, 11 AI-enabled tools in use

Executive summary

Meridian's staff adopted eleven AI-enabled tools over eighteen months without a centralized review. This assessment cataloged every tool, reviewed each vendor's data-training and retention terms, mapped where patient and business data flows, and produced a rationalization plan. Three tools present material exposure and should be reconfigured or replaced within 30 days. Consolidating four overlapping subscriptions recovers an estimated \$9,600 per year - more than the cost of this assessment.

11 AI tools cataloged	3 material exposures	\$9,600 annual savings identified	30 days to close critical gaps
---------------------------------	--------------------------------	---	--

1. Tool inventory and shadow AI discovery

Interviews with department leads, expense-report review, and single sign-on logs surfaced eleven AI-enabled tools. Four were unknown to ownership, including a browser extension summarizing patient intake forms and a personal ChatGPT account used for treatment-plan drafts.

Tool	Use	Data touched	Risk tier
ScribeAssist	Visit transcription	Patient health info	High
ChatGPT (personal)	Treatment-plan drafts	Patient health info	High
FormSnap extension	Intake summarization	Patient health info	High
SchedulAI	Appointment booking	Contact details	Moderate
CopyPilot	Marketing copy	None sensitive	Low

(Excerpt - the full inventory covers all eleven tools.)

2. Vendor data rights and contract review

Each vendor's terms of service, data-processing agreement, and sub-processor list were reviewed against five questions: Does the vendor train models on customer data? Is zero-data retention available? Where is data stored? Who are the sub-processors? What happens to data at termination?

- ScribeAssist trains on audio by default; the healthcare tier with a signed BAA and zero-retention mode is available at the current seat count for \$18/user/month more.
- The personal ChatGPT account has no business agreement in place. Drafts containing patient details are retained and may be used for training. This is the single largest exposure found.
- FormSnap's privacy policy permits sale of de-identified data to third parties. Its sub-processor list includes two analytics providers outside the United States.

3. Data flow and boundary mapping

Patient health information currently reaches four external AI services, two of which lack a business associate agreement. The map delivered with this report shows every system that touches patient data, the API boundaries involved, and where prompt logs and transcripts are retained.

4. Rationalization and cost takeout

Four subscriptions overlap: two transcription tools, two marketing copy tools. Consolidating onto the two vendors that passed the contract review recovers \$9,600 per year in seat and subscription costs and removes two data paths entirely.

Recommendations - first 30 days

- Move ScribeAssist to the healthcare tier with a signed BAA and zero-retention mode enabled.
- Prohibit patient details in personal AI accounts; provide a covered business account with training disabled.
- Remove the FormSnap extension and return to manual intake review until a compliant summarizer is selected.
- Consolidate the four overlapping subscriptions; cancel the two that failed review.

This sample is abridged. A full engagement includes the complete inventory, per-vendor scorecards, the data-flow map, and an executive playbook with owners and deadlines. Cijara Group LLC - cijaragroup.com - CustomerInquiry@cijaragroup.com