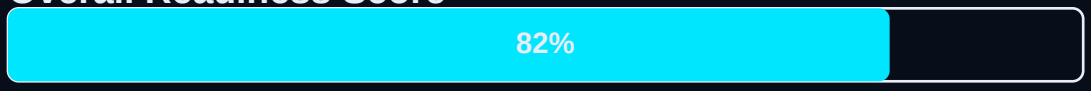
Client: PureGlow MedSpa

Date: October 23, 2025

Prepared by: SharpAudit AI Compliance Platform

This automated assessment maps HIPAA safeguards with NIST 800-53 and 800-171 control families.

Overall Readiness Score



Low Risk >80% | Moderate 60–79% | High Risk <60%

Executive Summary

PureGlow MedSpa demonstrates a strong overall compliance posture. Administrative and technical safeguards are largely implemented, with targeted improvements recommended for encryption at rest, vendor BAAs, and SIEM coverage. Addressing these gaps will raise readiness above 90% and reduce audit exposure.

Key Findings

Category	Finding	Impact	Severity
Access Control	Inactive user accounts remain enabled.	High	Moderate
Encryption	Stored PHI lacks AES-256 encryption at rest.	Critical	High
Audit Logs	SIEM coverage limited to 70% of endpoints.	Medium	Moderate
Vendor Risk	No signed BAAs for two third-party apps.	High	High
Training	Annual HIPAA training overdue for 3 staff.	Low	Low

Control Family Breakdown — HIPAA & NIST 800-53

Family	Status	Readiness %	Notes
Access Control (AC)	Implemented	88%	MFA enforced; review dormant accounts policy.
Audit & Accountability (AU)	Partial	76%	Increase log retention; centralize all endpoints in S
Security Assessment (CA)	Implemented	91%	Quarterly reviews in place; keep evidence snapsh
Configuration Mgmt (CM)	Partial	72%	Baseline hardening incomplete on macOS endpoi
Incident Response (IR)	Implemented	85%	Tabletop completed Q2; update contact tree.
Risk Assessment (RA)	Partial	70%	Vendor risk scoring not applied consistently.
System Integrity (SI)	Missing	55%	Missing EDR on legacy devices; patch cadence la

Legend: Implemented (≥80%), Partial (60–79%), Missing (<60%).

Risk Prioritization

Top risks: **Encryption gaps (at rest)**, **vendor BAAs** missing for two apps, **incomplete SIEM coverage** (approx. 30% endpoints not forwarding logs).

Remediation Roadmap

Action Item	Owner	Impact	Effort	Target
Enable AES-256 encryption for PHI storage	IT Lead	High	Medium	30 days
Review & renew vendor BAAs	Compliance Officer	High	Low	14 days
Expand SIEM coverage to 100%	Security Analyst	Medium	High	45 days
Reinstate HIPAA training	HR Manager	Low	Low	7 days
Deploy endpoint hardening baseline	IT Team	Medium	Medium	60 days

Quick Wins: BAAs, training. Strategic: encryption rollout, SIEM expansion, hardening baseline.