Sapphire Legal AI

Security & Compliance Whitepaper

Confidential — For Legal and IT Review

Executive Summary

Law firms increasingly handle sensitive client data but are experimenting with public AI tools that compromise confidentiality. Sapphire Legal AI is a private, practice-specific AI platform designed with privacy, security, and compliance at its core. Your data never leaves your environment, is never shared for training, and remains under your complete control.

Security Principles

- Complete Control — Deploy on-premises or private cloud
- End-to-End Encryption — AES-256 at rest, TLS 1.2+ in transit
- Zero Data Sharing — No data used for training or shared
- Least Privilege — Role-based access, SSO, SCIM
- Auditability — Comprehensive logging & SIEM export

Technical Architecture

Sapphire Legal AI operates entirely within the client ' s environment. Traffic enters through a private AI gateway with SSO integration, routes through the AI runtime (models + guardrails), and interacts only with encrypted storage and policy/audit layers. No egress to public internet for training or analytics.

Compliance Alignment

- SOC 2 Type II (roadmap)
- ISO 27001 (roadmap)
- HIPAA/HITECH alignment
- GDPR / CCPA adherence
- Data residency support for U.S., EU, UK, Canada

Key Security Features

- Access & Identity: SSO, MFA, RBAC, SCIM
- Data Protection: PII/PHI detection, redaction
- Logging & Monitoring: SIEM integration
- Resilience: Encrypted backups, configurable RPO/RTO
- Secure SDLC: Code scanning, signed builds

Risk Management

Threat modeling performed per deployment. Continuous vulnerability scanning, optional third-party penetration testing, and a shared responsibility model ensure robust security posture.

Customer Responsibilities

- Maintain secure infrastructure & IAM
- Enforce MFA for legal staff
- Conduct access audits regularly
- Use client-side encryption where required

Conclusion

Sapphire Legal AI provides confidentiality, integrity, and availability in a way public AI platforms cannot. By combining private AI runtimes with governance and auditability, firms can adopt AI safely without compromising trust.

Next Steps

Contact: info@sapphirelegal.ai
Schedule: www.sapphirelegal.ai/demo
Download: SIG-Lite package available on request