SETTLIT

SettLiT Security, Privacy, & Compliance Overview

At SettLiT, protecting sensitive medical and legal data is foundational to how we design, build, and operate our platform. We recognize that our clients trust us with highly confidential information, and we take that responsibility seriously.

Security First Architecture

SettLiT is built using a modern, security first cloud architecture designed to protect data at every stage of its lifecycle.

- Data encrypted in transit using TLS 1.2+
- Data encrypted at rest using industry standard AES 256 encryption
- Secure cloud infrastructure hosted with enterprise grade providers
- Role based access controls to ensure least privilege access

Access Controls & Identity Management

We tightly control who can access systems and data, and under what conditions.

- Role based user permissions aligned to job function
- Strong authentication requirements for internal users
- Environment access restricted to authorized personnel only
- Regular review of user access and permissions

Compliance & Regulatory Alignment

SettLiT operates in environments subject to strict legal, medical, and privacy requirements.

- HIPAA compliance reviewed with aligned controls and operational practices
- Designed to support compliance with healthcare data handling requirements
- Formal policies covering data handling, access, retention, and incident response
- Vendor and partner security review as part of onboarding

SOC 2 Readiness

SettLiT is actively working toward SOC 2 compliance.

- SOC 2 Type II readiness underway
- Controls mapped to Trust Services Criteria including Security, Availability, and confidentiality
- Internal audits and control testing in progress
- Ongoing documentation and process formalization

While SOC 2 certification is not yet complete, our security posture is designed to meet those standards today.

SETTLIT

Monitoring, Logging, and Incident Response

We proactively monitor systems to detect and respond to potential threats.

- Centralized logging and audit trails
- Continuous monitoring of system activity
- Defined incident response and escalation procedures
- Regular backup and recovery testing

Secure Development Practices

Security is embedded into how we build and ship software.

- Regular Third–Party penetration testing
- Secure software development lifecycle practices
- Code reviews and change management controls
- Separation of development, staging, and production environments
- Regular vulnerability and dependency management

SettLiT's Commitment to Security & Compliance

SettLiT is designed to meet the security and compliance expectations of law firms, healthcare partners, and enterprise clients handling sensitive medical data. Our current controls reflect SOC 2 level rigor, with formal certification in progress, and continuous investment in security as we scale.

Trusted by law firms that lead with speed and deliver results:

Dunn|Sheehan LLP

VALIENTE **M** MOTT

HALE LAW ACCIDENT ATTORNEYS

SS&H SCHECHTER SHAFFER & HARRIS, L.L.P. ACCIDENT & INJURY ATTORNEYS

Keller | Postman

ANAPOLWEISS

SS&H SCHECHTER SHAFFER & HARRIS, L.L.P. ACCIDENT & INJURY ATTORNEYS

D/C DUDDY & CZARNECKI

SBAITI & COMPANY

COWEN | RODRIGUEZ | PEACOCK
The Trucking Trial Lawyers