AI CLINICAL SCRIBE LLC Privacy & Security

The trust between doctors and patients stands as a paramount concern at AI CLINICAL SCRIBE LLC. We commit to adhering to HIPAA-compliant procedures for data storage and management for all information gathered and disseminated via the AI Clinical Scribe Platform.

Internal Personnel Security

Every AI CLINICAL SCRIBE LLC staff member must Undergo thorough background scrutiny prior to employment.

Annually complete training focused on security awareness, HIPAA, privacy, and data categorization.

Compliance

AI CLINICAL SCRIBE LLC regularly performs risk evaluations to ensure our policies are current and applicable.

Our Chief Technical Officer holds the responsibility for overseeing Privacy and Security measures.

Secure Development Lifecycle

Compliance checks are a must for all software modifications.

AI CLINICAL SCRIBE LLC employs an infrastructure-as-code approach, requiring all changes to the infrastructure to undergo scrutiny before implementation.

Engineers are mandated to undergo training in secure development Methodologies.

Cloud Hosting and Availability

Our hosting solutions and data handling are secured within Amazon Web Services (AWS) protected data centers.

Utilization of Amazon Web Services robust infrastructure guarantees uninterrupted data access.

Confidentiality and Data Encryption

Data protection measures include encryption both at-rest and during transit, adhering to recognized encryption protocols.

Vendor Management

Vendors involved in patient data processing must comply with HIPAA and enter into BAAs with AI CLINICAL SCRIBE LLC.

AI CLINICAL SCRIBE LLC continually assesses vendor security protocols to maintain stringent standards.

Artificial Intelligence

Compliance with HIPAA is ensured for all AI models, which do not retain data.

No protected health information is utilized in AI training.

Patient Information.

Encryption safeguards patient information both at-rest and in-transit.

Patient recordings are directly deleted post successful note creation without being stored on disk.

A 14-day retention period is in place for all patient data before its permanent deletion.