

DATA SECURITY & PRIVACY



ABOUT eLitigate[®]ZE

eLitigateZE is a secure, cloud-based virtual testimony platform that integrates Zoom-based video conferencing, exhibit management, and real-time speech-to-text to streamline legal proceedings. The platform can be accessed directly through any modern web browser, or seamlessly within Zoom as a dedicated, embedded Zoom App—providing flexibility for participants to join from their preferred environment. We follow industry best practices, conducting regular vulnerability assessments and penetration testing to maintain the highest security standards. Zoom provides end-to-end encryption options and robust administrative controls, ensuring that live video sessions are protected to enterprise-grade standards.

ENCRYPTED STREAMING

eLitigateZE media traffic is encrypted using AES-256 end-to-end encryption. This ensures streaming content remains secure, even over public networks.

NETWORK PROTECTION

Web traffic is secured with TLS 1.2, utilizing the strongest commercially available encryption protocols and cipher suites. Strong ciphers such as AES-GCM are used for encryption, with ECDHE providing Perfect Forward Secrecy and SHA-256/384 ensuring data integrity. All traffic is routed through an industry-standard Web Application Firewall (Cloudflare), which provides protection against Distributed Denial of Service (DDoS) attacks.

SECURE STORAGE

Access to testimony files is controlled through role-based and account-specific permissions. All case files—including exhibits, audio/video files, and transcripts—are stored on secure AWS cloud infrastructure with encrypted storage.

DATA COMPLIANCE

The eLitigateZE platform is hosted on AWS and follows Amazon's best practices for cloud security. Our solution complies with HIPAA requirements (we maintain a Business Associate Agreement with AWS) and has been certified under the EU-U.S. Privacy Shield.

We also prevent unauthorized data access through both server-side and client-side encryption, ensuring adherence to applicable regulatory requirements. For Amazon's SOC 3 report, please visit:

https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf

INFORMATION SECURITY

Esquire's Mission is to preserve and protect the sanctity of the record to ensure equal access to justice for all. For that reason, Esquire has been fanatically focused on protecting its clients' sensitive information with a security program closely aligned with the rigorous ISO 27001 framework. As a result, Esquire has successfully completed multiple AICPA SOC 2 Type II audits and recently upgraded its ISO 27001:2013 certification to the 27001:2022 standard.

AI & DATA USAGE

eLitigateZE does not use client data to train any generative AI models. When AI-based features are offered, they operate within strict data privacy guidelines:

- **No Model Training:** Data from proceedings, including testimony, exhibits, and transcripts, is never used to train or fine-tune AI systems.
- **Temporary Processing Only:** Any AI service provider used processes client data solely for the requested task, and is deleted after completion.
- **ASR Provider Privacy:** Our Automatic Speech Recognition provider processes audio solely to generate transcripts. The data is not retained, is deleted after processing, and is never used to improve or train speech models.
- **Confidentiality Maintained:** AI features are designed to meet the same security and compliance standards as the rest of the eLitigateZE platform, ensuring client confidentiality at all times.

