

# DATA SECURITY & PRIVACY



## ABOUT eLITIGATE

eLitigate is a cloud-based virtual testimony platform that combines video conferencing, exhibit management, and speech-to-text components to optimize the workflow of legal proceedings. In addition to conducting regular vulnerability assessments and penetration tests, eLitigate follows industry best practices.

## ENCRYPTED STREAMING

All eLitigate media traffic, audio and video, is encrypted using AES-256 encryption end to end. This industry-standard encryption means that streaming files are safe even on public networks.

## NETWORK PROTECTION

Web traffic is encrypted using TLS1.2 with the strongest commercially available encryption protocols and cipher suites. Industry standard WAF (Cloudflare) proxies all traffic to the application protecting against DDOS.

## SECURE STORAGE

Appropriate permissions to access testimony files for individual proceedings are role-based and account-specific. All testimony files e.g., exhibits, audio/video files, etc. are stored on secured cloud (AWS) servers leveraging encrypted storage; dedicated, standalone storage options are also available.

## DATA COMPLIANCE

The eLitigate platform is deployed on in the AWS cloud according to Amazon best practices. Our solution is implemented in the Amazon cloud according to our security program to ensure compliance with HIPAA regulations (we have a BAA on file with AWS) and has been certified under the EU-US Privacy Shield.

Additionally, eLitigate automatically blocks unauthorized users from accessing data via both server-side and client-side encryption, all while enabling cloud-related regulatory compliance. For the most recent SOC report from Amazon AWS please visit:

[https://d1.awsstatic.com/whitepapers/compliance/AWS\\_SOC3.pdf](https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf)