



Lexbe maintains state-of-the-art security to ensure that customer documents are never compromised. Data security is our top priority and our redundant infrastructure, multi-level application controls, and strong 256-bit SSL encryption deliver the highest levels of protection for your legal electronic stored information (ESI).

World Class Data Center Infrastructure

Lexbe operates within the Amazon Web Service (AWS) cloud environment and incorporates Amazon's Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), and Elastic Block Store (EBS) technology. Amazon is a leading service provider for the infrastructure, network, and physical security layers of a cloud-based network environment. Servers are maintained in secure, limited access, physically isolated data centers, and monitored from network operating centers 24x365. AWS data center personnel do not have logical access to Lexbe applications or to the data of any Lexbe customers hosted online.

Document and Data Encryption

Lexbe only uses the strongest security when managing your case data. We transmit and store your ESI using strong 256-bit (AES-256) encryption, the same technology used by leading financial institutions.

Proactive Network Intrusion Monitoring

We operate redundant firewalls to protect our servers and your data from potentially malicious network traffic. We also use Network Intrusion Detection Service (NIDS) technology to monitor network traffic, and to detect, report and respond to anomalies, which are indicative of a network-based attack. This may involve taking proactive counter-measures when a network attack is detected; including denial of service (DOS) attacks and other potential malicious traffic or incursions at the network layer.

Reliability and Backup

We configure all servers and networking components in a redundant configuration for persistent reliability. Our uptime over the last 5 years exceeds 99.995% and we provide customers a 99.99% uptime guarantee. All customer data is stored redundantly in multiple separate data centers and syncing/downloads occur daily. In a disaster, we are configured to be able to restore client data from remotely stored back-ups. Clients additionally can periodically download their own files and data for an additional level of redundancy, if desired.

You Own the Data; Confidentiality

Our Terms of Service disclaim any ownership interest in your and your client’s documents and data. We acknowledge that we hold subject to your attorney-client and work-product privileges.

Audits and Certifications

Our data centers provide Service Organization Controls 1 & 2 reports published under SSAE 16 and ISAE 3402 professional standards (formerly SAS70 Type II audits). We enable HIPAA covered entities to leverage our secure environment to process, maintain, and store protected health information. Additionally, our data centers have achieved ISO 27001 certification, and have been successfully validated as a Level 1 service provider under the PCI Data Security Standard (DSS).

