Everlaw

Security and Compliance Overview

Compliance and Security of Customer Data

As a provider of cutting-edge software for customers with highly confidential data, we recognize how important security is to protecting information. We understand that the security of our product and the compliance-oriented culture of our business are instrumental in maintaining the trust our customers place in us, and we are committed to protecting that information.

Everlaw's compliance program is holistic. It demonstrates not only our abidance by the laws and regulations regarding security and confidentiality, but our commitment to our customers, to professional ethics, and to our company values.

The framework for compliance at Everlaw has seven elements:
1. Risk assessment, monitoring, and third-party audits
2. Everlaw Code of Conduct, Policies and Procedures
3. Oversight by our CEO and Board, and accountability resting with our Director of Compliance
4. Human resources security practices and appropriate delegation of authority
5. Education, communication, and awareness for the entire Everlaw team
6. Enforcement, discipline, and incentives
7. Continuous improvement

Cloud Service Provider and Data Center Security

Our primary data source is stored on secure Amazon Web Services (AWS) cloud servers, which surpass industry standards for privacy and security. AWS has SOC 1, 2, and 3, ISO 27001, FedRAMP, and FIPS certifications, in addition to meeting compliance standards for many other legal and security frameworks. You can read more about AWS' compliance practices and certifications here: https://aws.amazon.com/compliance/.

Third Party Auditing

At Everlaw, we routinely undergo rigorous security testing of our entire security infrastructure by an independent third party auditor. Undergoing examinations of this nature, rather than solely relying on the credentials of our cloud service provider, illustrates Everlaw's ongoing commitment to creating and maintaining the most stringent controls for the protection and security of our customers' confidential information.

SOC 2 Type 2 Certification and HIPAA Compliance

Everlaw has its own SOC 2 Type 2 certification in Security, Availability, and Confidentiality. We've also been audited for compliance with HIPAA.

For a company to receive SOC 2 Type 2 certification, it must have sufficient policies and strategies that satisfactorily protect customers' data, and it must provide detailed evidence and pass independent testing of their operational effectiveness through the audit testing procedures. We are happy to provide a copy of the SOC 2 Type 2 audit report to customers or prospective customers upon request.

System Availability

On average over an annual basis, our uptime exceeds 99.9%, including scheduled maintenance windows.

Low-level Access Controls and Intrusion Detection
All data is encrypted in transit via TLS and at rest using AES-256. We use intrusion detection software to monitor our servers for break-ins. We are notified immediately if there is any unexpected activity. Our servers are firewalled to prevent external access via any ports other than 80 (http) and 443 (https). We use key-only (no passwords) and multi-factor authentication for low-level server access to prevent password-guessing. We also impose IP address restrictions limited to our office to prevent third parties from accessing our servers.

Access Controls
We employ state-of-the-art practices to prevent cross-site scripting and cross-site request forgery. Access to data can be restricted by user or security group. All user activity is fully logged on the system. We store when a user has logged in and logged out, and every action he or she has taken on the site—down to which pages of which documents he or she has viewed. This information is visible both to us and to administrators on the case, so any suspicious activity can be detected and acted upon quickly.

When two-factor authentication is activated for a case, users are required to authenticate every computer or device through which they access Everlaw by providing both their password and another piece of information. The second factor can either be a one-time code delivered to their email address, or a rolling Google Authenticator app on their mobile device.

Application Security
Everlaw's Application Development Policy requires that our engineers employ information security steps to ensure the protection of sensitive information, application availability, and data integrity. The Everlaw application servers respond only to SSL-encrypted HTTP calls. Our SSL certificates are signed by an industry-leading certificate authority and are signed with a minimum 1024-bit encryption.

Data Collection and Privacy
Except as required to provide the service or as otherwise required by law, we do not disclose data to any third party. We do not store any information not expressly provided by users, regardless of whether their browser sends a "Do Not Track" signal.

Data Backup
Data is stored in triplicate in different AWS geographical locations, with 99.999999999% yearly durability. User work product is backed up in this same fashion six times a day. Recovery is provided as part of Amazon's cloud offerings.

Data Retention, Return, and Destruction
Unless otherwise specified, we purge all copies of any user data at the conclusion of the case. That includes local, cloud, and original media. When a customer requests deletion, Everlaw destroys the media and deletes the case from the servers. We issue deletes to the Amazon S3 storage layer of the relevant resources and retry deletes to ensure that all deletes succeed. All document images, text, and metadata are deleted. Everlaw complies with contractual requirements to provide proof of deletion.

Security Incident Management and Breach Policy
Everlaw's Incident Reporting and Response Policy contains a procedure for incident management, with a clear escalation path to the Director of Compliance and CEO and steps for breach notification. We are insured in case a loss of data causes our users economic harm. Should such an event occur due to our negligence, we would immediately put steps

in place to minimize the damages and to improve our processes. Should such a breach occur as a result of malicious behavior by an employee of Everlaw, that person would be immediately released and his or her access to the platform revoked.

Regulatory Compliance
Everlaw's compliance program includes regular monitoring and evaluation of compliance with applicable laws and regulations, as well as employee training. Everlaw complies with HIPAA, and undergoes independent examination regarding our HIPAA compliance procedures. As such, we will review and sign Business Associate Agreements upon request.

Our compliance program also includes training for all employees on important regulatory and compliance issues regarding Anti-Money Laundering, Antitrust, and Gifts & Entertainment.

Employee Security Policies and Practices

Below are some of our key internal security and compliance policies and practices.

Everlaw's Operations
Everlaw's office space is monitored by CCTV and secured by an alarm system with cameras at each entry point. The premises are locked at all times and our employees access the premises using individually-monitored electronic key fobs. Visitors to our office must be escorted and logged, and we retain these logs indefinitely.

Everlaw requires full disk hard drive encryption and multi-factor authentication for all employee computers. We control employee access to customer data using role-based access and account management. The Director of Compliance monitors all employee access requests and changes.

All of our employees (we do not have any contractors) are required to undergo background checks and sign our confidentiality agreement upon hiring. We also require employees to follow Everlaw's Code of Conduct, Information Security Policies, and Business Policies, which are covered during compliance training.

Governance
Protecting confidential data is our top priority. Our compliance program at Everlaw includes regular meetings of our Risk Committee and Security Management Team, led by our Director of Compliance, and include our CEO and members of each team at Everlaw. The Risk Committee and Security Management Team work together on Everlaw's Business Continuity Plan and Disaster Recovery Procedure, which is tested every year. Everlaw employees complete compliance training upon hiring, face-to-face security and compliance training at least annually, and additional security training on relevant topics, such as the OWASP Top Ten.

We hope that our continuing commitment to security, as well as our transparency regarding policies and practices, set your mind at ease. If you have any more questions about Everlaw's security, don't hesitate to contact us.