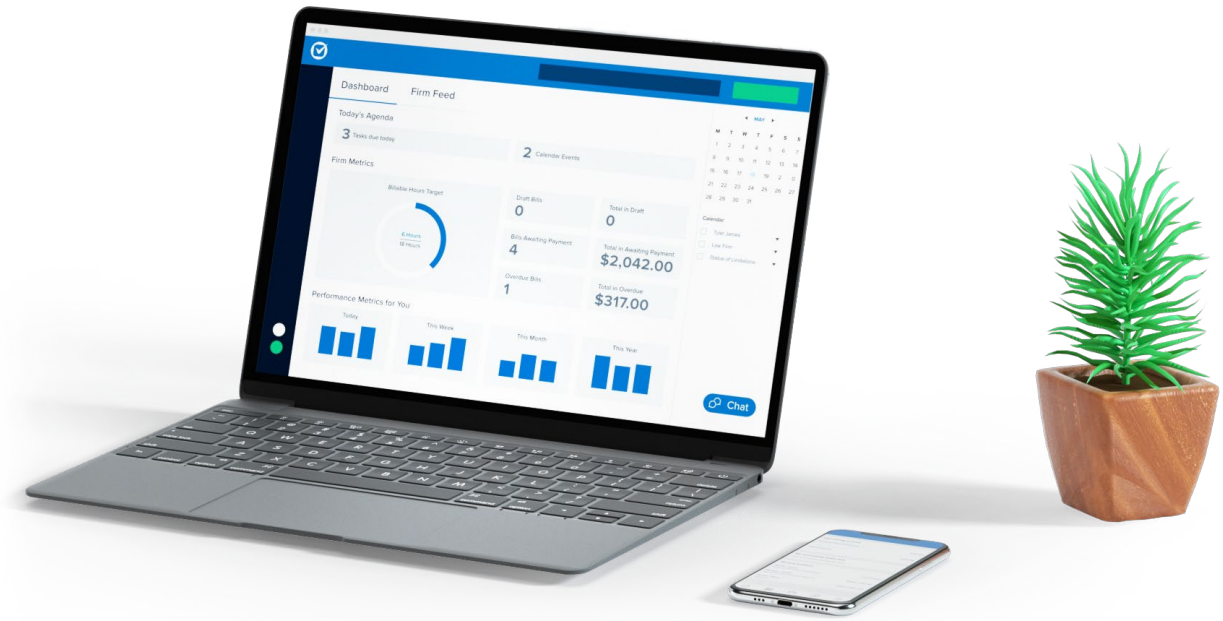
A Rundown on Clio's Security Protocols and Infrastructure

Protect your clients' information and firm's data with top security features and protocols. Here are the measures Clio takes to keep your information secure.



Application Security

We have implemented automated and custom checks using industry leading auditing tools, processes to track, triage, and apply security patches, and industry-standard host- and network-level security protections (i.e. firewalls, configuration integrity, change management, etc.) to ensure that Clio is protected from common web vulnerabilities and other known security threats. Additional information can be found in Security and Reliability.

Clio also operates a bug bounty program through security@clio.com. Considered a technology industry standard, we set up independent security researchers, who come with different perspectives, testing methods, and experiences, with separate test accounts to analyze and report on any potential security concerns.

In addition to this, we also undergo an annual penetration test by a globally respected security consultancy.

Encryption

Clio encrypts data both at-rest and in-transit using 256-bit AES encryption for SSL/TLS web traffic and 2048 bit RSA public keys. We use a combination of Software Based Encryption, hosting solutions (Amazon Web Services and Google Cloud Platform) and Secure Self Encrypting Devices to align with NIST Special Publication 800-53.

You can verify these settings using the following links:

Manage (US) Manage (EU) Manage (CA) Grow (US)

User Authentication

Clio follows industry best practices for user authentication. We use bcrypt (a password hashing function) to store Clio user passwords, and an automatically scaling bcrypt cost factor to ensure our password storage keeps up with Moore's Law. We also apply filters to ensure passwords can never show up in our log files.

We use rate limiting to restrict login attempts based on defined thresholds. Our servers log every access attempt with full details (i.e. userID, IP address, date/time, result), and are monitored for failures. Repeated authentication failures are automatically blacklisted.

Account Administrators are able to enforce the use of strong passwords and Multi-Factor Authentication (MFA) through Google Authenticator or the Clio App if desired for all users using the Clio service.

Employee Security

We take on a rigorous review process to ensure that anyone joining Clio has the necessary competencies and expertise to do their jobs (including comprehensive pre-employment screening).

We enforce the use of strong passwords and Multi-Factor Authentication (MFA) wherever possible.

We recognize the importance of training and require all staff to undergo security, compliance, and data privacy training on a regular basis. This includes onboarding training for all new staff and annual refresher training for all employees. Our goal is to increase awareness around these concepts and embed them in everything we do.

Hosting

All Clio data centers are SOC2 certified, and employ the strictest physical and logical security—including CCTV cameras, onsite security personnel, motion sensors, biometric ID cards, and other security measures. Our data centers only provide access and information to employees and contractors who have a legitimate business need based upon the principle of Least Privilege. All visitors and contractors are required to present identification upon entry, and are escorted continually by authorized staff while onsite.

If you'd like to learn more about the security practices of Clio's hosting providers, please refer to the following links:

AWS

Security Practices
Security Compliance

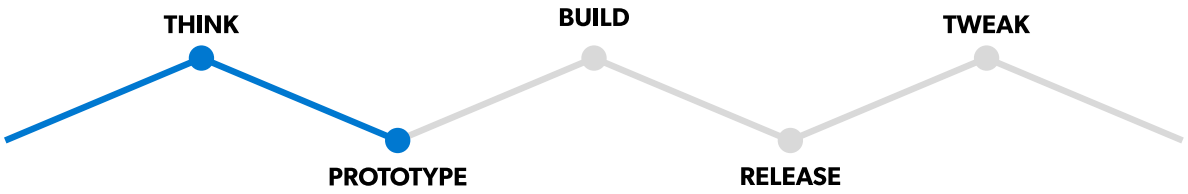
GCP

Security Practices
Security Compliance

Software Development

We embed security best practices into every step of our development lifecycle. These practices include, but are not limited to, manual and automated code reviews and internal compliance scans. Clio also works with external security researchers to ensure that our products meet the highest quality and security criteria.

Here's an outline of our Software Development Life Cycle (SDLC) process:



Incident Management

Clio is prepared to respond to any security incident. We have a simple process we follow to address the incident at hand, communicate effectively (both internally and externally), and to prevent future incidents.

Our incident response process aligns with NIST SP 800-61. Refer to the image for a high-level overview.

As per our Terms of Service, Clio will notify customers within 72 hours of identifying an incident which impacts their information. We are committed to ensuring we comply with all applicable laws and regulations.

Business Continuity

Clio has implemented a business continuity strategy leveraging geographically redundant data centres, data replication, and full/incremental backups. Clio customers may also choose to implement our data escrow service, which performs regular backups to Amazon's S3 service or implement Clio's 'recovery bin' service, which permits the potential recovery of previously deleted items.

Compliance

Clio is committed to maintaining the privacy of all information collected, processed, and/or stored on its users and employees. Beyond complying with regulatory requirements (such as GDPR), Clio values the privacy and security of its users and aims to govern the use and protection of information accordingly. At Clio, we design our products, services, and processes according to the tenets of Privacy By Design, along with ascribing to fair information principles (as outlined in applicable legislation such as the GDPR, CCPA, and PIPEDA). Additionally, Clio undergoes an annual assessment as part of TRUSTe's Enterprise Privacy & Data Governance Practices certification program.

We utilize hosting providers with services located in the United States, Canada, and the European Economic Area (EEA) to store and process the data we collect from you and abide by any data residency requirements for these locations. All of these locations have been assessed to ensure appropriate data protection laws are in place to protect your information. Please refer to our Privacy Policy to learn more about the types of information we handle, how we use that information, and your associated rights.

Clio currently utilizes third-party service providers to support its PCI-DSS compliance efforts. Clio leverages Stripe to facilitate credit card payments from its subscribers, and LawPay to process payments within the application for its users' clients.

Learn more about the security practices of Clio's payment processors below:

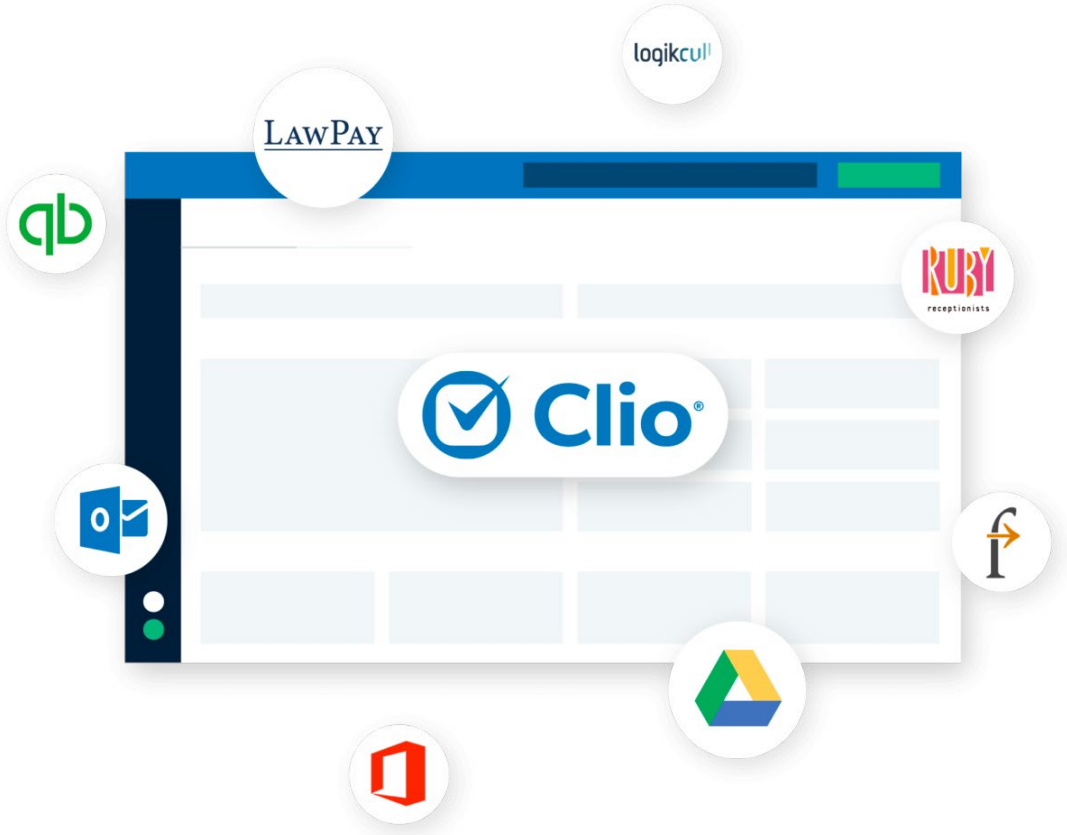
LawPay
AN AFFINIPAY SOLUTION

Security at LawPay

stripe

Security at Stripe

While Clio does not currently sign Business Associate Agreements, a number of our supported integrations—Dropbox, Box, Office 365, NetDocuments, and Google Drive—support this compliance requirement.



API & Integrations

Clio's open API is supported by industry-standard OAuth 2.0, access restricted by OAuth 2.0 "Scopes," and governed by Clio's Developer Terms of Service. All integrations must be directly authorized at the User-level offering visibility and control. Further information about Clio's Third Party integrations can be found in Clio's App Directory and Terms of Service.

Additional Questions?

Clio has a dedicated team of security professionals that would be happy to answer any questions you might have. Please reach out to Customer Support at support@clio.com or call **1-888-858-CLIO** to speak with a member of our team.

All product names, trademarks and registered trademarks are property of their respective owners. All company, product and service names used in this document are for identification purposes only. Use of these names, trademarks, and brands does not imply endorsement.