Themis Solutions Inc.

State Bar of California Due Diligence Questionnaire

Where are your primary servers located?

Clio's primary data center is in located Illinois, and redundant data centers are located throughout the continental US. For security reasons Clio does not disclose the full address of its data centers.

Where are your back-up servers located?

All of our back-up servers are located within the continental United States. For security reasons Clio does not disclose the full address of its data centers. Up to 4 separate and geographically redundant data centers back-up the information stored in Clio in real time.

Are there redundant power supplies for the servers?

All critical systems at Clio have full redundant fail-overs, including servers, power, network and HVAC systems.

How often, and in what manner, is users' data backed up?

Backups of users data are performed continually in real time. Backups of systems, including operating systems and source code files, are performed daily.

What are the regulatory requirements in the jurisdiction where the servers are located?

Clio's primary datacenter is located in Illinois; all Clio datacenters are subject to US law.

Do you engage in cross-jurisdictional or cross-border data transfers? If so, when and where? Will you be notified?

Clio does not actively engage in cross-border data transfers. However, the nature of least-cost routing for all Internet communications does not guarantee that data transferred through any Internet service (including email and all other web-based applications) will remain in the United States.

Is there a compliance plan for cross-jurisdictional or cross-border transfers? Do you employ Tier 4, 256-bit encryption, bank-level security?

All of Clio's data transmissions are protected using 256-bit SSL encryption, providing bank-grade data protection. Clio's server infrastructure undergoes extensive daily security audits and penetration testing. Clio's data centers undergo routine audits verifying physical and logical security as required by SSAE 16 SOC 1.

What types of encryption methods are used and how are passwords stored? How are passwords protected?

Data in transit is always protected by 256-bit SSL at a minimum. Private keys are kept in a secure (encrypted) key repository and available only to those who require them to carry out their duties (i.e. operations staff who manage them on the application servers).

Passwords are encrypted using an irreversible salted digest.

Are these security measures in place both while the data is in transition and in storage?

All data is encrypted while in transit. Sensitive information, such as passwords and credit card information, is encrypted at rest. Clio's data center data handling procedures adhere to PCI-DSS regulations

Database backups that are sent off-site are secured via GPG public/private key encryption; the private keys are stored only in our secure key repository and nowhere else, except for temporary installation on a host if it becomes necessary to restore a database backup (and therefore a private key is required to decrypt that backup). After the backup has been restored, the private key is immediately removed from the system.

Have your operations ever been audited? If so, can we have a copy of the report?

Clio's data centers are all SSAE 16 SOC 1 audited. Clio also has a number of third party audits performed in various capacities, including network security, application penetration testing, and business continuity planning and testing (in addition to other audits). This documentation is considered confidential.

What is your annual server uptime? If any reports exist regarding uptime for the past few years, can we have copies?

Our annual server uptime exceeds 99.9%. Real-time reporting on Clio's status is available at status.goclio.com.

Do you own your servers, or lease them from a 3rd-party?

Clio leases servers and computing resources from SSAE 16 SOC 1 audited third parties.

If you lease them, can we have a copy of the 3rd-party agreement?

This information is confidential.

Will our data be stored on a dedicated server, or on a multi-tenancy server?

Clio utilizes multi-tenant data infrastructure.

If multi-tenant, how is our data segregated from others?

Clio uses best practice data normalization strategies and application-level controls to ensure secure isolation of customer data.

How is the server building physically secured?

Clio's data centers are SSAE 16 SOC 1 data centers that employ the strictest and physical and logical security:

- All premises are closely monitored and guarded, 24x7x365, with sophisticated pan/tilt CCTV covering every part of the facility and security guards posted at all entrances.

- Access to servers is restricted to a limited number of authorized engineers.

- Security is strictly enforced using the latest technology, including man-trap technology between lobby and datacenter, motion sensors and biometric controlled ID key-cards.

What is your policy regarding employee access to stored data?
Each employee is given the absolute minimum amount of access required to fulfill their required duties. Database access is highly restricted, and only permitted as required by the most tenured members of the operations team.

Clio employees will only access or read your data for the purposes of troubleshooting or diagnosing an issue. Such access would always require your explicit consent by providing your username and password. Data center employees do not have the ability to access or read your data.

What kind of training is provided your employees?

We offer unlimited access to customer support via live agent or email.

Have you ever had a security breach?

Clio has never had a security breach.

What is your customer notification policy upon breach? What is your response policy upon breach? What is your disaster recovery/business continuity plan?

Any unauthorized access of Clio's systems would constitute a significant security incident. In the event of such an occurrence, Clio would act immediately to ensure information security, and would subsequently work to determine the magnitude of the incident and inform all parties affected.

What is your protocol concerning access to and exportation of our data?

Using Clio's Data Escrow facility, users can keep an up-to-date copy of firm information in an AWS account. Users can also perform an any-time data export to a local device on demand by visiting app.goclio.com/export. Data tables are available for export in open source (comma delimited) formats/

What is your company's history -- e.g., how long have you been in business, and where do you derive your funding?

Clio was originally developed with the advise of the Law Society of British Columbia in 2007.

Are you Safe-Harbor certified?

Clio has not sought out Safe Harbor certification to date. All data centers are SSAE 16 SOC 1 audited.

Can we have a copy of your Service Level Agreement (SLA) to review?

Yes; Clio's User License Agreement and SLA are accessible to all users.

How do you respond to 3rd-party subpoenas?

Per our terms of service and privacy policy, we maintain that our primary duty is to protect client information to the extent the law allows. Were we provided a subpoena to release client information we would contact the affected parties and afford them opportunity to legally intervene to protect client information before disclosing any data without authorization. Additionally, given that we are a Canadian company, subpoenas would need to be enforceable under Canadian law in order to require our compliance.

Do you attempt to claim full/shared ownership of our data upon transfer to your facilities?

No; per our terms of service and privacy policy, users data remains the property of the Clio account owner or a named administrator.

Do you carry Cyber Insurance to cover losses resulting from a data breach, including 1st-party and 3rd-party coverage?

Clio has secured liability insurance to provide coverage against deliberate or accidental damages.

Can our data also be backed up to a third party backup service?

Using Clio's Data Escrow facility, users can keep an up-to-date copy of firm information stored in an Amazon Web Services (AWS) S3 account. The service is available at no additional charge from Clio and a nominal storage rental fee with Amazon.