31 Short Questions Attorneys Must Ask About the Cloud

Donna Seyle – Lawyer/Writer/Founder at LawPracticeStrategy.com
Perry L. Segal – Attorney at Charon Law, SP

Checklist: Vetting the Vendor

When considering which virtual law practice vendor to choose, it is essential to conduct due diligence regarding the vendor's security and other practices to insure that legal and ethical obligations may be met. These security measures must insure that the confidentiality of client data will be maintained by identifying various security protocols a vendor follows for content, in transmission or at rest. There are other ethical issues that arise when using off-premise technology, such as the cloud, that need to be addressed with your vendor. The following is a list of pertinent questions the attorney – or the attorney's technical staff/vendors must answer when vetting the firm's virtual law practice vendors:

Virtual Law Office (VLO) Checklist

- Where are the primary servers located?
- Where are the back-up servers located?
- Are there redundant power supplies for the servers?
- How often, and in what manner, is users' data backed up?
- What are the regulatory requirements in the jurisdiction where the servers are located?
- Do they engage in cross-jurisdictional or cross-border data transfers? If so, when and where? Will you be notified?
- Is there a compliance plan for cross-jurisdictional or cross-border transfers?
- Do they employ Tier 4, 256-bit encryption, bank-level security?
- What types of encryption methods are used and how are passwords stored?
- How are passwords protected?
- Are these security measures in place both while the data is in transition and in storage?

Virtual Law Office (VLO) Checklist

- Have their operations ever been audited? (If so, obtain a copy of the report).
- What is their annual server uptime? (Obtain a copy of the report for as many years as possible).
- Do they own their servers, or lease them from a 3rd-party?
- If they lease them, what are the terms of the 3rd-party agreement? (Obtain a copy).
- Will your data be stored on a dedicated server, or on a multi-tenancy server?
- If multi-tenant, how is your data segregated from others?
- How is the server building physically secured?
- What is their policy regarding employee access to stored data?
- What kind of training is provided their employees?
- Have they ever had a security breach?
- What is their customer notification policy upon breach?
- What is their response policy upon breach?

Virtual Law Office (VLO) Checklist

- What is their disaster recovery/business continuity plan?
- What is their protocol concerning access to and exportation of your data?
- What is the company's history—e.g., how long have they been in business, and where do they derive their funding?
- Are they Safe-Harbor certified? (Insures that their security measures comply with the EU Directive, a comprehensive regulatory scheme). Not necessary, but comfortable.
- Ask for a copy of their Service Level Agreement (SLA) to review.
- How do they respond to 3rd-party subpoenas?
- Do they attempt to claim full/shared ownership of your data upon transfer to their facilities?
- Do they carry Cyber Insurance to cover losses resulting from a data breach, including 1st-party and 3rd-party coverage?