LEGALfuel
The Practice Resource Center of The Florida Bar

Quick Start Guide on Cloud Computing

I want to move to and work in the cloud. What does that mean?

There are two primary ways you can use the cloud: (1) cloud storage; and (2) cloud-based applications. Also known as SaaS (software as a service), cloud storage means that your files are stored on someone else's server in some other location and you remotely access those files. It gives us the ability to share large files, backup and sync files across multiple computers, and undelete things. Working in the cloud allows lawyers to grow or shrink a practice without having to buy storage servers and enter IT maintenance contracts. It also gives you flexibility by allowing you to access files remotely from your phone or from home and spend fewer days in the office. Platform as a service means that your applications (e.g., Microsoft Word, Excel, and PowerPoint) are cloud-based – they are stored in the cloud and you can log into them from anywhere.

Where is my[1] data really? Is it backed up at a second location?

This is called "geographic redundancy" (i.e., the same data located in more than one location). This is standard in the industry. You should inquire as to where the data is housed, as there may be privacy or data security laws (data localization laws) or contractual obligations with certain clients that limit where the data may be maintained (CSP Due Diligence Standards I.C.).

Is my data encrypted? Or, can someone read my data if it gets stolen? Make sure you ask your provider if they test or hack their own system to make sure it is safe (like secret shoppers!).

Encryption makes data "unreadable" and is one of the most powerful technical safeguards used to minimize the risk of unauthorized access to sensitive information. It is important that access to the encryption key (which can be used to unlock and read the encrypted data) is limited. It's also important to know who your key is being shared with when evaluating providers. (CSP Due Diligence Standards II.A. and II.B.)

Will you share my information with third parties? Will you tell me if you do?

Given the sensitive nature of the data (client information, personal information, and proprietary information), it is reasonable to request that no third-party have access to your data or encryption keys for the data, and that your provider give you notice if it changes who has access to the data. (CSP Due Diligence Standards II.A., II.C., and IV.F.)

---

[1] *Well, my and my clients' data.

You might be holding my data, but I want it to be only mine!

It is important that you have ownership rights in your data. When one of the parties wants to terminate the relationship, you should be able to request a copy of all your data and require that the provider permanently and securely delete your data. If not, you may be obligated to inform your client of the possibility that the client's data "may linger on the cloud provider's servers for a period after representation has ended." (CSP Due Diligence Standards II.D. and IV.E.)

I want to be sure that when someone accesses this data you make them prove who they are.

Find out what type(s) of end user authentication the provider uses. "End User Authentication" is the way the provider determines you are who you say you are when you try to access data. This can be done by using simple login credentials (username and password), or it could be done with a stronger safeguard like two-factor authentication (e.g., receive a text message with a PIN) or biometrics (e.g., fingerprints or facial recognition through your mobile device). (CSP Due Diligence Standards III.A.)

How many times a month do you crash or do scheduled maintenance causing my data to become inaccessible (uptime/downtime)? I'm looking for a long-term, reliable relationship here.

Maintenance and other technical issues could make your data inaccessible. This is known as "downtime." Cloud service providers should offer a service level agreement with an "uptime guarantee" of 99.9% to 99.999% and assurances that maintenance is performed during off-peak hours. They should also provide information on their track record of meeting their uptime guarantee and regular, public notifications of downtime. (CSP Due Diligence Standards IV.A. and IV.C.)

What is a data breach and how do I prevent one?

A data breach occurs when an unauthorized person gains access to sensitive, protected, or confidential data. This includes confidential client information and personal information (e.g., SSNs, medical records, financial data, etc.). You can reduce your chances of experiencing a data breach by taking advantage of your provider's two-factor authentication and encryption. Make sure that your provider has a privacy policy and that it will isolate your data. Also, make sure that you can monitor who is logging into your account and when. (CSP Due Diligence Standards III.C., IV.B., IV.D., and IV.G.)

What if something happens to my data? How do you handle it? What will you tell me?

Your provider should have a process in place to notify you within 48 hours of discovering a data breach. It should also explain any costs or obligations you may bear because of a data breach and explain what indemnification or insurance coverage it may provide to you. In the event of a disaster, the provider should have in place a plan for protecting and recovering your data. The terms of the provider's service agreement should also outline any limitations on your ability to access data, whether the provider will indemnify you if it accidentally destroys or alters your data, and your payment terms. (CSP Due Diligence Standards III.E., IV.G., and IV.H.)

How do I know you're a provider I can trust?

There are several industry standards and certifications that are common in the cloud computing industry. These standards and certifications address security, privacy, and confidentiality: (CSP Due Diligence Standards I.B.)

- Service Organization Controls ("SOC") Type 2 report on security, availability, processing integrity, confidentiality, and privacy
- International Standardization Organization ("ISO") 27001 certification on information security management
- ISO 27018 certification on protection of information in the cloud
- Legal Cloud Computing Association standards on cloud computing

Are you in compliance with any applicable federal, state, or industry-based security and privacy legal frameworks?

Depending on the content of the data being stored, the provider may need to comply with one or more legal frameworks. Examples of these frameworks are: (CSP Due Diligence Standards I.B.)

- The Payment Card Industry's Data Security Standards (PCI);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy Rule, Security Rule, and Breach Notification Rule under HIPAA;
- Gramm-Leach-Bliley; and
- The Sarbanes-Oxley Act (SOX).