In recent years, an increasingly large number of law firms have moved their software and data to the cloud. In fact, the ABA reported that the percentage of lawyers who use cloud-based software and services jumped from 21 percent in 2012 to 31 percent in 2013!

If you’re one of the many lawyers who have decided to take advantage of the cloud for cost savings, mobility, security, flexibility and disaster preparedness, it’s important that you do your research and ask the right questions to ensure you select a service provider that will help you meet the highest standards for your ethical obligations, client service and efficiency.
MISTAKE #1

Not Knowing Where Your Data Really Lives

The ABA has recently ruled cloud computing ethical so long as lawyers take “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

How does this relate to data storage?

You need to know where your data will be stored because depending on the geographic location of your cloud provider, and the locations of their data centers, it may fall under different regulations. Be particularly cautious if a vendor uses data centers located outside of the United States, as laws regarding privacy may vary.

The Pennsylvania Bar Association, in Formal Opinion 2011-2000, suggests that lawyers exercising reasonable care should ensure their providers “will host the firm’s data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania.”

Many Public Cloud and SaaS providers hide the ‘how’ and ‘where’ of data storage deep within a service agreement. Chances are, the provider doesn’t actually host your data as many providers use third-party data centers located throughout the world. This poses a variety of potential problems including security, confidentiality and level of service.

A good way to ensure you know where your data is at all times is to use a dedicated cloud solution instead of a Public Cloud or SaaS application.
MISTAKE #2

Assuming You Own Your Data

Many Software-as-a-Service (Saas) and Public Cloud vendors have been known to claim that all data uploaded into their system is their property—an unacceptable scenario when it comes to your confidential case and client files.

In 2011, Dropbox briefly updated its terms of service to include language that permitted Dropbox ownership rights over its users’ data when stored in the cloud. Ownership quickly reverted back to the users in response to public outcry, as Dropbox backpedaled to explain to users that it only needed access for administrative purposes.

Your service agreement should explicitly state that you retain ownership of all data that is stored on the cloud server(s). This ensures that you’ll always be able to access your case and client data in the event that you terminate your relationship with the cloud provider or should they go out of business.
MISTAKE #3

Neglecting to Integrate All of Your Systems

One of the biggest draws to the cloud is the ability to use any device, from anywhere, to access your data. While many lawyers use the cloud for their practice management platform, they neglect to integrate all other systems.

What about your email? Word processing? Research tools? In order to gain maximum productivity, you should be able to access your entire practice from anywhere. With a complete private cloud solution, you can create, edit and collaborate on documents in real-time with both colleagues and clients. You can leverage from different applications that converge under a single remote environment making it easy to perform efficiently.

Additionally, with a fully integrated private cloud solution, you can ensure the highest level of security, backup and disaster preparedness for all of your applications and data – not just the data relevant to your case management platform.
MISTAKE #4

Relying on Multiple Parties for Support & Maintenance

Imagine this: You can’t access your firm’s website and you call your hosting company. They tell you it’s not them, but your Internet Service Provider (ISP). You call your ISP and they can’t find a problem and tell you to contact your DNS management company. With DNS on the phone, they tell you it’s not them, but your hosting company. Does this sound familiar?

Having multiple vendors means there are multiple points of failure, and everyone can point the finger at someone else. All this does is prevent you from resolving your issue quickly, and easily, so you can get back to billable activities.

When selecting a cloud provider, it’s advisable to choose a company that offers full IT management so they can shoulder the burdens of system maintenance, security updates and software upgrades for you. In case of a problem, you know exactly who to call.

Other benefits of a fully managed cloud solution include:

- Managed antivirus and malware protection
- Automatic and managed back ups
- 24x7 monitoring
- Firewall and intrusion prevention
- Automatic software upgrades
MISTAKE #5

Focusing Solely on Price, Disregarding Best Practices

It’s quite common: Businesses in every industry see a low price and get excited about potential cost savings, neglecting to realize the long-term implications of choosing a subpar service and vendor.

It’s easy to see a low price and get sucked in to thinking you’ll save money, when in reality you’re putting your firm in grave danger of losing or inadvertently sharing confidential client and case data and violating ethical rules and regulations.

While there are cloud vendors offering service for only pennies on the dollar per month, these services do not include Best Practices for Cloud Technology such as 5 tiers of security, a OC2/SSAE16 certified Data Center, inherent redundancy and disaster recovery, managed backups, 99.999% uptime guarantees and more.

While Service Level Agreements (SLA) from different vendors may sound similar, the resulting uptime (or lack-thereof) is vastly different. For example, a 99.9% SLA says that you may experience almost 9 hours of downtime per year, while a 99.999% SLA guarantees no more than 5 minutes of downtime per year!
CONCLUSION

Not All Clouds Are Created Equal

When choosing a cloud provider, look for a vendor that specializes in the legal industry so you know they understand your specific requirements and can meet your needs when it comes to ethical obligations and client service levels.

If you’ve been thinking about changing how your law firm currently operates, we can help you assess and explore all possible options with a Technology Readiness Assessment. Let us help you determine if a virtual office or an in-house solution would be best for your firm. In either case, we will consult and design a custom tailored solution that we’ll then deploy and manage for you so you can focus on what you do best: Practicing Law!

GET A FREE DISASTER RECOVERY AUDIT!
1-888-994-8615
apc@abacusnext.com