Cloud Technology and Remote Workforces

In the wake of the pandemic, the adoption of cloud technology and remote workforces in the legal sector is accelerating, prompting lawyers and law firms to manage new and emerging risks.

There will always be growing pains during a digital transformation. Lawyers will have to navigate bugs and technical difficulties, technologies will be discontinued or replaced, and hackers and scammers will try to exploit new security vulnerabilities.

And the level of risk will vary. A glitch that caused a lawyer to appear as a cat during an online court session led to embarrassment. But security vulnerabilities such as malware, ransomware, or a data breach could lead to more serious consequences for lawyers.

It's important to take these risks into account when transitioning to cloud technology and remote workforces.

What to Know About Cloud Technology

Cloud technology refers to the many kinds of technology software and services available to businesses remotely. Vendor companies will offer law firms and other businesses the use of "cloud" services, including offsite document storage services and law practice management software, on a pay-as-you-go basis, also known as "software as a service" (SaaS).

These documents and software live "in the cloud," making your firm's data securely accessible from any location. Many cloud software-as-a-service vendors also offer law practice management software applications for email, calendaring, integrated billing and client management, easily facilitating your remote workforce management.

LOCKTON AFFINITY LAWYER

What the Cloud Can Offer Law Firms

Cloud technology offers many benefits to businesses, particularly those with remote workforces. Among the chief benefits for law firms are:

- **Cost Savings**—Reduced cost and capital expenditures means that firms no longer need onsite computer data storage equipment. Instead, data stored in the cloud is accessible from any computer, tablet or other device with access to the internet.
- **Flexibility**—Increased flexibility and scalability of storage and access needs means that firms pay only for the number of users that need access, easily accommodating downsizing or growth cycles.
- **Data Accessibility**—The on-the-go portability of data across different devices means that firms no longer need to create or maintain multiple versions of the same document on multiple devices.
- **Secure Collaboration**—Sharing and collaborating on document reviews and revisions with clients is easier in the cloud, where documents can be saved to a shared folder and viewed by a client with secured password access.

What Risks and Obligations Lawyers Face

Due to the unique nature of the legal profession, law firms employing cloud technology for their remote workforces face additional risks that other business sectors do not. Legal obligations to exercise due diligence, protect attorney-client privilege and safeguard technical systems and data will apply.

Lawyers using cloud technology and law firms working remotely should consider key ethical implications. ABA Model Rule 1.6 states that a lawyer "shall not reveal information relating to the representation of a client without the client's informed consent." Model Rule 1.15 is the basis of an attorney's duty to safeguard clients' property entrusted to counsel.

Several state ethics opinions offer insight into lawyers' obligations to their clients when engaging the services of cloud technology vendors, consistently noting that lawyers must exercise "reasonable care to protect the security and confidentiality of client documents and information."

Further opinions have stated this "reasonable" standard requires lawyers become knowledgeable[1] about pertinent technologies and take reasonable care to stay abreast[2] of technological advances.

How Law Firms Can Manage the Risk

There are steps that lawyers and law firms can take to minimize the chance of loss or exposure of sensitive documents and information through malware, ransomware, data breach or other security vulnerabilities.

When engaging with third-party cloud technology providers, lawyers should take time to carefully review the vendor's Service Level Agreement and use the following risk control techniques to help manage the ethical and professional risks:

1. Verify the vendor's business model, financial stability, background and their procedures for data handling should the vendor go out of business.
2. Ensure the vendor conforms to the highest industry standards for data security, data encryption and security audit procedures.
3. Confirm that your firm will own your data and all its rights.
4. Ensure the vendor won't have access that jeopardizes the attorney-client privilege.
5. Confirm that the vendor will assume responsibility and legal liability for data confidentiality and that there are no liability limitations for a breach.
6. Ensure the vendor's compliance with HIPAA, the HITECH Act and other state and federal privacy and confidentiality laws.
7. Verify the physical location of the vendor's data storage facilities and equipment and review the vendor's choice of law provision in the Service Level Agreement.
8. Determine whether and how you will be able to control levels of access for lawyers, support staff and clients.
9. Confirm procedures for contract termination, ensuring that your data will be returned to your firm in a usable format with the vendor's copies subsequently and permanently deleted from servers.
10. Inquire about other representative clients of the vendor, such as corporations in data-sensitive industries and, ideally, other law firms.

LOCKTON AFFINITY LAWYER

Cloud technology and remote workforces are here to stay for the foreseeable future. New innovations that allow for greater mobility and connectivity can positively impact the legal profession. But make sure you understand the added level of risk and additional obligations lawyers and law firms face. Review your ethical and professional obligations when using cloud technology and do your due diligence when choosing to work with third-party cloud technology vendors.

Discover more benefits of cyber and professional liability insurance today here or give us a call for a free, no obligation consultation at (844) 398-0465

1 California State Bar Standing Committee on Professional Responsibility and Conduct, Formal Opinion 2010-179; Florida Bar Standing Committee on Professional Ethics, Opinion 06-01 (April 10, 2006); Illinois State Bar Association Ethics Opinion 10-01 (July 2009); The Maine Board of Overseers of the Bar Professional Ethics Commission, Opinion 194 (June 30, 2008); Massachusetts Bar Association Ethics Opinion 05-04 (March 2005); The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 33 (Feb. 9, 2006); The New Jersey State Bar Association Advisory Committee on Professional Ethics Opinion 701 (April 2006); State Bar Association of North Dakota Ethics Committee Opinion 99-03 (June 21, 1999); Vermont Bar Association Advisory Ethics Opinion 2003-03; Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (September 30, 2005).

2 See Alabama Office of General Council Disciplinary Commission, Ethics Opinion 2010-02; State Bar of Arizona Ethics Opinion 09-04 (December 2009); New York State Bar's Committee on Professional Ethics issued Opinion 842 (Sept. 10, 2010); North Carolina State Bar Ethics Committee Formal Opinion 6 (currently under further review); Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2011-200.