CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Caution in the Cumulus: Lawyers' Professional & Ethical Risks and Obligations Using the "Cloud" in Their Practice

A CNA PROFESSIONAL COUNSEL GUIDE FOR LAWYERS AND LAW FIRMS

CLOUD COMPUTING – AN OVERVIEW

Lawyers are increasingly looking to cloud computing as a way to increase the efficiency of their firms' practice management as well as for document storage solutions. While cloud computing is reshaping law practice management, lawyers must recognize and manage the related risks inherent in this new technology.

Vendors offering "cloud services" provide document storage services as well as access to law practice management software on a pay-as-you-go basis.[1] These services store documents in the cloud, making them available from any secured device from any location. In addition to offering document management solutions, "cloud" vendors also offer a number of law practice management applications such as email, calendaring, integrated billing programs and client management tools.

The purpose of this article is to provide an overview of the advertised benefits that cloud vendors are marketing to law firms and to raise awareness of inherent risks that lawyers must address before taking their practice to the "cloud."

While cloud computing is reshaping law practice management, lawyers must recognize and manage the related risks inherent in this new technology.

THE POTENTIAL BENEFITS OF CLOUD COMPUTING FOR LAW PRACTICE MANAGEMENT

Numerous companies are now offering cloud-based services focused specifically on the needs of law firms.[2] These cloud vendors market various benefits in seeking to move law practice management functions to their cloud. These benefits include the following:

1. Reduced Cost/Reduced Capital Expenditures

By using cloud computing, attorneys and law firms will no longer need computers with large memories, external hard drives, or servers to store all of their data. Instead, this information would be stored in the cloud and would be accessible from any computer, tablet or other device with access to the Internet.

2. Scalability/Flexibility

Another benefit of cloud computing is that law firms only pay for their actual usage of the service. For example, if the law firm needs access for ten users, the firm pays for ten users. If, within six months, the firm has downsized and only needs six users, the firm only pays for six users. Alternatively, if within one year the firm has experienced growth and needs 15 users, the firm can pay for access for 15 users.

3. Accessibility of Data Across Different Devices

Cloud computing and storage also eliminate the need to create multiple versions of the same document on multiple devices. If a document was stored in the cloud, an attorney could draft a document on his or her work computer and then update the same document from his or her personal tablet or laptop from home.

4. Sharing/Collaboration

Finally, the most compelling feature of storing documents in the cloud is the ability to collaborate on those documents. For example, when an attorney assists his or her client in responding to written discovery, those documents must be reviewed by the client. Often, the method to assist the client requires emailing revised versions of the document back-and-forth and saving those emails (and attachments) in your email program and in the client file. By utilizing the cloud service, attorneys can simply save the document to a shared folder and provide the client with secured password access to the folder containing the document.

1 There are many other technical aspects of "cloud computing." This article will focus solely on cloud computing as it relates to vendors who offer document storage services as well as developed law practice management programs, sometimes referred to as "software as a service" or "SaaS."

2 See Appendix A – Non-Exclusive List of Cloud Vendors and Websites.

ETHICAL IMPLICATIONS OF USING THE CLOUD IN LAW PRACTICE

The two ethical rules implicated when engaging a cloud vendor are ABA Model Rules 1.6 and 1.15.[3] Rule 1.6 states that a lawyer "shall not reveal information relating to the representation of a client without the client's informed consent." Rule 1.15 is the basis of an attorney's duty to safeguard clients' property entrusted to counsel.

As set forth above, the very essence of cloud computing is the uploading of information onto a third-party's network of servers. Therefore, it is imperative that attorneys recognize the risks associated with utilizing this new technology. They also must keep abreast of the current trends in ethics opinions in their jurisdiction relating to the use of cloud computing.

A number of state ethics opinions have offered insight into lawyers' ethical obligations to their clients when engaging the services of cloud vendors.[4] These ethics opinions are consistent in their admonition that lawyers must exercise "reasonable care to protect the security and confidentiality of client documents and information" when using cloud based services. The Arizona and New York opinions go one step further, stating that this "reasonable" standard requires attorneys to keep abreast of current technologies to ensure that the storage system remains sufficiently advanced to protect the client's information.

In other jurisdictions, ethics opinions have addressed the use of other technologies such as wireless computing, electronic filings, emails and the use of off-site network administrators.[5] The premise of those opinions is analogous to the use of cloud computing, recognizing that attorneys must be knowledgeable about the pertinent technology and take reasonable care to uphold the rules of professional responsibility in using the technology.

Accordingly, attorneys should first become educated about cloud computing and the potential risks associated with the use of the technology. The following discussion is intended to raise awareness of risk control issues relating to the use of cloud computing in order to provide a basic level of education for attorneys who are interested in utilizing this technology.

RISKS OF MOVING TO A CLOUD STORAGE SYSTEM

While cloud computing offers a number of compelling benefits associated with law practice management, a number of risks also arise in using cloud technology in the rendering of legal services.

Attorneys should address all foreseeable risks and ethical issues with their cloud vendor prior to contracting for its services. Lawyers also should consider risks unique to their specific areas of legal practice, as well as unique to their state's laws and rules of professional conduct, when contracting for cloud services. One of the best means of addressing those risks with the cloud vendor is in the Service Level Agreement ("SLA").

When engaging a cloud vendor, the most important document that a law firm will review will be the SLA. Many of these SLAs are less than one page and address only the "uptime" of the cloud provider. "Uptime" is a term indicating that the cloud vendor guarantees that the attorney will have uninterrupted access to information in the cloud. Most cloud vendors will guarantee approximately 99.999% uptime.[6]

Many current vendors that market their services to law firms will probably have more relevant language in their SLAs, while cloud vendors that do not focus on the legal profession will likely have general and vendor-biased agreements. Irrespective of the vendor's focus, attorneys should review the terms and conditions of the SLA in the context of compliance with all applicable laws and rules of professional conduct.

While the SLA is not always negotiable, vendors will sometimes entertain reasonable negotiations concerning the terms and conditions of the SLA.[7] If the SLA does not provide the law firm or your clients with the necessary security and protections, review other available resources for pursuing this technology. Attorneys should not engage any vendor whose terms would be "unreasonable" or attempt to disclaim or limit liability for its own errors, omissions or neglect.

3 Note that the ABA Model Rules provide the basis for the rules of professional conduct in most states, but are not binding. Lawyers should review the applicable rules of professional conduct in their respective jurisdiction for further guidance.

4 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.

5 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).

6 See also the term "FIVE NINES", which refers to a provider offering 99.999% uptime. It is the "gold standard" in utility service industries. See Cloud Computing Opinion: *The Goal of "Five Nines" – 99.999% Availability is Meaningless,* Ajax World Magazine, Sept. 15, 2008 at **http://ca.sys-con.com/node/674934**.

7 See Appendix B – Service Level Agreement ("SLA") Language Samples for Lawyers Using Cloud Computing.

RISK CONTROL TECHNIQUES FOR MANAGING THE RISKS OF CLOUD COMPUTING AND STORAGE

Lawyers and law firms who have decided to contract with a cloud vendor should use the following risk control techniques to help manage the ethical and professional risks when using cloud services.[8]

- *Who is the Vendor?* Attorneys should investigate the vendor. What is the vendor's business model? Is the vendor financially stable?
- *Ownership of Data.* Attorneys should confirm that the law firm will be the sole owner of data and that the vendor has no ownership or other rights to the data.
- *Confidentiality of Data.* Attorneys should confirm that the vendor will assume responsibility and legal liability for confidentiality of data.[9]
- *Location of Data Storage.* Attorneys should confirm the location of data storage. Attorneys should review the choice of law provision in concert with laws that may govern the situs of data storage.
- *How is System Usage Logged/Accessed?* Can the law firm define and control different levels of access to certain files for various employees/clients? Accessibility can be important if the firm must apply different security and access for lawyers and support staff .
- *Exit Strategy: Return of Data/Deletion Upon Termination.* Attorneys should confirm that the vendor will return data to the firm in a usable format. For example, if the law firm stored Microsoft Word documents with the vendor, is the data returned in that format or another format that is unusable to the law firm? In addition, confirm that the vendor will ensure that upon return of data, it is permanently deleted from the vendor's servers.
- *Confirm Vendor's Full Acceptance of Liability.* Confirm that there are no limitations on the vendor's liability.
- *Who are Some Representative Clients?* If the cloud vendor is reputable, the vendor typically will have relationships with other corporations in data-sensitive industries and, ideally, other law firms.
- *Obtain the Client's Consent to the Use of Cloud Storage.* Attorneys should explain to the client that the firm uses cloud storage in the practice. In addition, attorneys should always obtain the written consent of the client to the use of cloud storage of client files and documents. The consent should be in writing and signed by the client.[10]

CONCLUSION

While cloud computing can be attractive for many reasons, lawyers should not participate in order to simply adopt the latest technology. In fact, cloud computing might not be beneficial for all law practices, depending upon the needs of the practice.

Instead, lawyers should conduct a reasonable review of the current model of their law practice management and evaluate whether a move to the cloud would be beneficial. If the law practice would benefit from the advantages offered by cloud computing, then the appropriate steps must be taken to ensure that the law firm fulfills all of its ethical and business obligations to its clients.

8 See Appendix D – Cloud Vendor Checklist.
9 Lawyers may continue to be bound by the applicable rules of professional conduct regardless of third-party contract terms.
10 See Appendix C – Client Consent to Use of Cloud Storage

Appendix A

NON-EXCLUSIVE LIST OF CLOUD VENDORS[11]

- Appirio: **http://www.appirio.com**
- Citrix: **http://www.citrix.com/lang/English/home.asp**
- Clio: **http://www.goclio.com**
- Dialawg: **https://www.dialawg.com**
- HoudiniESQ: **http://houdiniesq.com**
- IntraLinks: **http://www.intralinks.com**
- Livia: **http://www.livialegal.com**
- Merrill Lextranet: **http://www.merrillcorp.com**
- MyCase: **http://www.mycaseinc.com**
- Next Point: **http://www.nextpoint.com/**
- Rocket Matter: **http://www.rocketmatter.com**
- Thomson Elite: **http://www.elite.com**
- Total Attorneys, LLC: **http://www.totalattorneys.com/**

11 CNA does not endorse, recommend, or make any representations or warranties as to the accuracy, completeness, effectiveness, suitability, or performance of any of the companies, websites, products, applications, software, or programs identified herein. The names are provided simply as a reference.

Appendix B

SERVICE LEVEL AGREEMENT ("SLA") SAMPLE PROVISIONS FOR LAWYERS USING CLOUD COMPUTING

The Service Level Agreement ("SLA") is the most important document that an attorney will review and eventually sign in order to engage a vendor for cloud computing. It is critical to carefully review all SLA terms and conditions to protect the law firm and its clients' rights *and* comply with all applicable professional and ethical obligations.

The following SLA language samples[12] are for informational purposes only and are not intended to be comprehensive.[13] Cloud vendors may be amenable to changing the terms and conditions in the SLA. Attorneys should review the SLA sample provisions to help draft SLA terms and conditions that comply with applicable laws and rules of professional conduct. In addition, attorneys should ensure that a vendor does not attempt to disclaim or limit liability for its own errors, omissions, and neglect.

I. PHYSICAL SECURITY

[Vendor] will ensure the presence of professional security at the computer server hosting facilities at all times.

II. OWNERSHIP OF DATA

Example 1

Other than the rights and interests expressly set forth in this Agreement, and excluding works derived from [Vendor], [User] hereby reserves all right, title and interest (including all intellectual property and proprietary rights) in and to [User's Content].

Upon request by [User] made before or within thirty (30) days after the effective date of termination, [Vendor] will make available to [User] for a complete and secure (i.e. encrypted and appropriate[ly] authenticated) download file of [User's Content] in [User's Choice of] format including all transformation definitions and/or delimited text files as well as attachments in their native format.

Example 2

The parties agree that upon the authorized termination of this Agreement, the [Vendor] and any subprocessor shall, at the option of the [User], return all the personal data transferred and the copies thereof to the [User] or shall destroy all the personal data and certify to the [User] that it has done so, unless legislation imposed upon the [User] prevents [Vendor] or subprocessor from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will ensure the confidentiality of the personal data transferred and will not actively process the personal data transferred.

The [Vendor] and the subprocessor warrant that upon request of the [User] and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to above.

III. DUTY IN EVENT OF BREACH

[Vendor] shall report in writing to [User] any use or disclosure of [User's Data] not authorized by this Agreement or in writing by [User], including any reasonable belief that an unauthorized individual has accessed [User's Data]. [Vendor] shall make the report to [User] immediately upon discovery of the unauthorized disclosure, but in no event more than two (2) business days after [Vendor] reasonably believes there has been such unauthorized use or disclosure. [Vendor]'s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) reasonably identify the [User's Data] disclosed, (iii) the identity of the party responsible for the unauthorized disclosure, (iv) what [Vendor] has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure of [User's Data], and (v) what corrective action [Vendor] has taken or shall take to prevent future similar unauthorized use or disclosure. [Vendor] shall provide such other information, including a written report, as reasonably requested by [User].

12 See similar and other examples at **http://www.educause.edu/wiki/Cloud+Computing+Contracts**.

13 These sample SLA provisions are for illustrative purposes only. The SLA you enter may present different terms and conditions from those noted in the sample. We encourage you to modify the SLA to suit your individual practice and client needs. As each law practice presents unique situations, and statutes and regulations may vary by jurisdiction, we recommend that you review in accordance with such state laws prior to use of this or similar SLAs in your law practice.

Each party acknowledges that, in the course of performance hereunder, they may receive personally identifiable information that may be restricted from disclosure under federal and state laws and regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and/or Health Information Technology for Economic and Clinical Health (HITECH) Act and/or the Sarbanes-Oxley Act of 2002 (SOX). Notwithstanding any other provision of this Agreement, each party will be responsible for all damages, fines and corrective action arising from disclosure of such information caused by such party's breach of its data security or confidentiality provisions pursuant to such laws and regulations as set forth herein.

IV. STORAGE LOCATION, VENUE AND CHOICE OF LAW

[Vendor] agrees to store and process [User's Data] only in the continental United States. The terms of this Agreement are entered into in the State of _____, and all duties and responsibilities of the parties that arise under this Agreement will arise under the legal obligations and authorities of the State of _____. At times, [Vendor] may store [User]'s data at a location outside of the State of _____ in furtherance of [Vendor]'s business purposes. If [Vendor] stores [User's] data at a location outside of the State of _____, it is expressly [Vendor's] responsibility that the other state will maintain the data in compliance with all federal laws, the terms of this Agreement, and the laws of the State of _____. Regardless of the location of [User]'s data at the time of any breach of this Agreement, the Parties' duties and responsibilities as set forth in this Agreement shall be defined by the State of _____ and any action brought to enforce those rights and duties shall be brought in the _____ in the State of _____.

V. CONFIDENTIALITY

Where a [Vendor] is required to disclose the [User's Data]] pursuant to the order of a court or administrative body of competent jurisdiction or a government agency, the [Vendor] shall: (i) if practicable and permitted by law, notify the [User] prior to such disclosure, and as soon as possible after such order; (ii) cooperate with the [User] (at the [User]'s costs and expense) in the event that the [User] elects to legally contest, request confidential treatment, or otherwise attempt to avoid or limit such disclosure; (iii) limit such disclosure to the extent legally permissible and (iv) notify [User] immediately after disclosure of all facts relating to the disclosure including, but not limited to, the identity of the requesting body, the name, address and phone number of a contact from the requesting body, and specifically identify each and every piece of [User's Data] that was disclosed pursuant to such judicial or administrative body order.

VI. AUDIT OF VENDOR

[Vendor] agrees to have an independent third party security audit performed at least once each year. The audit results and [Vendor]'s plan for addressing or resolving of the audit results shall be disclosed to [User] within ___ (X) days of the [Vendor]'s receipt of the audit results. The audit should minimally check for buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other vulnerabilities.

VII. LIMITED ASSIGNMENT OF VENDOR'S OBLIGATION IN EVENT OF CHANGE IN OWNERSHIP

This Agreement shall be binding on the parties and their successors (through merger, acquisition or other process) and permitted assigns. Neither party may assign, delegate or otherwise transfer its obligations or rights under this Agreement to a third party without the prior written consent of the other party.

[In addition, your SLA might want to address the event that your Vendor goes out of business. SaaS escrow services from "brick and mortar" document storage companies have begun to address the concern that a cloud computing vendor will go out of business, so you might want to consider negotiating to include escrow language in your contract.]

Appendix C

DRAFT LETTER ADVISING CLIENT OF USE OF CLOUD STORAGE

Client Important
Address
Re: Notice of Use of Cloud Storage

The Law Office of Ms. Attorney is pleased to use the services of Cloud Vendor X as its document management and document storage provider. All documents exchanged between you and our firm during the course of representation may be scanned and stored in a personal and confidential file with Cloud Vendor X. All documents will be maintained in a confidential manner in accordance with our firm's rights and obligations to you as our client. This letter is intended to inform you of our firm's relationship with this third-party vendor in order to provide full disclosure regarding the location in which your file materials will be stored during the course of this representation.

Your signature below confirms that this information has been discussed with you and that you have no objection to The Law Office of Ms. Attorney's use of Cloud Vendor X for its document management and document storage provider.

Very truly yours,

Ms. Attorney

Acknowledged and Agreed to:
Signature:_____
Printed Name:_____
Title: _____
Date:_____

Appendix D

CLOUD VENDOR CHECKLIST

CLOUD VENDOR INFORMATION	YES	NO	COMMENTS IF NO OR NOT APPLICABLE
1.1 Has the attorney investigated the background of the vendor?			
1.2 Is the vendor financially stable?			
1.3 Is the attorney satisfied with the vendor's business model?			
1.4 Has the attorney confirmed that the vendor utilizes security audits?			
1.5 Has the attorney requested a copy of the security audits?			
OWNERSHIP OF DATA			
2.1 Has the attorney confirmed that the law firm is the sole owner of the data and that the vendor has no rights to the data?			
2.2 Has the attorney confirmed that the vendor has no rights to access documents that may jeopardize the attorney-client privilege?			
CONFIDENTIALITY OF DATA			
3.1 Has the attorney confirmed that the vendor will assume responsibility and legal liability for the confidentiality of data?			
3.2 Has the attorney confirmed the means by which the vendor will keep the data secure (firewall, encryption, etc.)?			
3.3 Has the attorney confirmed that the vendor agrees to comply with state and federal privacy and confidentiality laws and regulations concerning document storage, including but not limited to HIPAA and the HITECH Act?			
FORMAT OF DATA			
4.1 Has the attorney confirmed that the firm will have access to raw data in the original file format (for authenticity purposes for litigators, etc.)?			
LOCATION OF DATA STORAGE			
5.1 Has the attorney confirmed the location where the data will actually be stored?			
5.2 Has the attorney reviewed the choice of law provision in the SLA?			

continued on next page

CLOUD VENDOR CHECKLIST *(continued)*

SYSTEM USAGE, LOGGING AND ACCESS	YES	NO	COMMENTS IF NO OR NOT APPLICABLE
6.1 Can the law firm define and control different levels of access to certain files for different employees/clients (Important for firms that have different security and access for lawyers and support staff)?			
EXIT STRATEGY: RETURN OF DATA/WIPE UPON TERMINATION			
7.1 Has the attorney confirmed that the vendor will return data to the firm in a usable format (For example, if the law firm stored Microsoft Word documents with the vendor, is the data returned in that format or another format that is unusable to the law firm)?			
7.2 Has the attorney confirmed that the vendor will ensure that once data is returned that it is permanently deleted from the vendor's servers?			
CONFIRM VENDOR'S FULL ACCEPTANCE OF LIABILITY FOR BREACH			
8.1 Has the attorney confirmed that there are no limitations on liability for the vendor?			
WHAT HAPPENS IF THE VENDOR GOES OUT OF BUSINESS?			
9.1 Has the attorney confirmed with vendor what happens to the data if the vendor goes out of business?			
WHO ARE SOME REPRESENTATIVE CLIENTS OF VENDOR?			
10.1 Has the attorney inquired as to the vendor's relationships with other corporations in data-sensitive industries and, ideally, other law firms?			

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com.