

# **CLOUD COMPUTING AND THE ETHICAL CHALLENGES**

Prepared for Multi-Track Federal Criminal Defense Seminar:  
Strategies for Defending Complex Cases

**AOKI LAW PLLC**  
Russell M. Aoki  
Coordinating Discovery Attorney

## **I. INTRODUCTION**

Cloud computing can raise ethical concerns for attorneys because confidential client information is stored by third party service providers. The American Bar Association described cloud computing as software accessed via the internet that allows data to be stored remotely by a vendor rather than on the computer of an attorney or law firm(also referred to as “Software as a Service” or SaaS for short)<sup>1</sup>.

Nineteen state bar associations have written ethics opinions on its member’s responsibilities while using cloud computing services. Each of the nineteen opinions holds attorneys to a duty of “reasonable care” though the requirements of reasonable care vary with each state. A summary of the opinions is outlined below with the full ethics opinions attached.

## **II. SUMMARY OF STATE ETHICAL OPINIONS**

### **Alabama**

The Alabama Disciplinary Commission drafted an opinion concluding attorneys should use reasonable care when using cloud computing. Reasonable care requires the attorney “to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement.” Any breach of confidentiality because of cloud-computing or third-party file storage will be evaluated on “whether the attorney acted reasonably in selecting the method of storage and/or the third party provider.” Attachment A.

### **Arizona**

In 2005 the Committee on the Rules of Professional Conduct (“the Committee”) published an advisory opinion in response to a member’s question on whether client files could be stored on computers with access to the internet. The Committee determined it was ethical so long as the attorney and firm take “competent and reasonable steps to assure that the client’s confidence are not disclosed to third parties through theft or inadvertence” and “take reasonable and competent steps to assure that the client’s electronic information is not lost or destroyed.” Attachment B.

---

<sup>1</sup> See Legal Technology Resource Center, *Cloud Computing/Software as a Service for Attorneys*, AM. BAR ASS’N, [http://www.americanbar.org/groups/departments\\_offices/legal\\_technology\\_resources/resources/charts\\_fyis/cloud-ethics-chart.html](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html) (visited June 9, 2014).

Most recently in 2009 the Committee published an opinion that it was permissible to create a system for clients to access and view documents online so long as attorneys took “reasonable precautions to protect the security and confidentiality of client documents and information”. The Committee noted changes in technology would require attorneys to periodically review the security measures. Attachment C.

### **California**

The State Bar of California Standing Committee on Professional Responsibility and Conduct (“the Committee”) was presented with the question of whether an attorney violates the duties of confidentiality and competence by transmitting or storing confidential client information with the use of technology. The Committee concluded any breach of duty would “depend on the particular technology being used and the circumstances surrounding such use.” Specific factors that should be considered include the degree of sensitivity of the information and the level of security provided by the technology. Attachment D.

### **Connecticut**

The permissibility of using cloud computing in the practice of law was addressed by the Connecticut Bar Association’s Professional Ethics Committee “(the Committee)”. The Committee emphasized the importance of the attorney taking “reasonable efforts to prevent unauthorized access to or disclosure of such data.” Attachment E.

### **Florida**

In a 2013 opinion, the Professional Ethics Committee published an opinion later affirmed by its Board of Governors that “attorneys may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security and that the attorney has adequate access to the information stored remotely.” It was also recommended that attorneys using cloud computing services research the provider. The opinion relies heavily on Iowa and New York’s previously published opinions. Attachment F.

### **Iowa**

The Iowa State Bar Association Committee on Ethics and Practice Guidelines determined the rules of professional conduct permitted attorneys to use cloud computing so long as the attorney performs “due diligence to assess the degree of protection that will be needed and to act accordingly.” The Committee provided a

preliminary list of questions the attorney should ask regarding accessibility of the data and data protection. Attachment G.

### **Maine**

In response to a question posed by its members as to whether it was ethical for Maine attorneys to use cloud computing, the Professional Ethics Committee concluded the use of cloud computing was permissible and provided a detailed list of procedures and policies attorneys should use to comply with the code of professional conduct. The conclusion reached by the Committee was an “attorney must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information...” Attachment H.

### **Massachusetts**

In a 2013 ethics opinion, the Massachusetts Bar concluded attorneys could use internet based storage “so *long as* the attorney undertakes reasonable efforts” to ensure the practices and procedures of service providers are compatible with the attorney’s ethical obligations. The opinion includes a list of items which would constitute a “reasonable effort” on the part of the attorney including review of the provider’s data privacy policies. Attachment I.

### **Nevada**

In 2006, the State Bar of Nevada Standing Committee on Ethics and Professional Responsibility concluded attorneys can comply with their ethical obligations and store client information electronically so long as they act “competently and reasonably to ensure the confidentiality of the information”. Attorneys are advised to exercise reasonable care in the selection of the service provider, have an expectation that the information will be kept confidential, and instruct the service provided to keep the client information confidential. Attachment J.

### **New Hampshire**

The New Hampshire Bar Association Ethics Committee published an opinion confirming attorneys could use cloud computing “as long as the attorney takes reasonable steps to ensure that sensitive client information remains confidential.” A list of specific issues which an attorney must consider before using cloud computing was provided. The questions included whether the service provider was a reputable organization, the level of security measures provided, and whether there was a disaster recovery plan for stored data. Attachment K.

### **New Jersey**

The Advisory Committee on Professional Ethics for the New Jersey Bar Association published an opinion in response to a member asking whether an electronic filing system was permissible. The opinion concluded using an electronic filing system was acceptable as long as original copies of documents deemed “client property” were kept in paper format (ex: wills, executed contracts, and corporate bylaws). As with paper files, an attorney has the obligation to exercise reasonable care “against the possibility of unauthorized access to client information.” Attachment L.

### **New York**

In response to a question as to whether an attorney may use an online system to store client files, the New York State Bar Association Committee on Professional Ethics concluded RPC 1.6 was not violated so long as an attorney used “reasonable care to ensure that confidentiality will be maintained”. Reasonable care may include investigating the service provider’s security measures, ability to purge client information, and whether there is an enforceable obligation to preserve confidentiality. Attachment M.

### **North Carolina**

North Carolina’s State Bar Ethics Committee published a formal ethics opinion in 2012 after receiving multiple inquiries regarding the ethical implications of contracting with software vendors. The opinion concluded that “if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files” then an attorney may use cloud computing services. The Committee declined to identify what specific security requirements were required to meet the “reasonable care” standard and instead required “due diligence and frequent and regular education”. Attachment N.

### **Ohio**

The Ohio State Bar Association Professionalism Committee concluded the use of cloud computing to store a client’s data was permissible. The opinion emphasized four main considerations when determining if cloud computing was appropriate: competent selection of a vendor; preserving confidentiality of the client’s data; supervising vendors; and communicating with the client. Attachment O.

### **Oregon**

A formal opinion concluding attorneys could contract with third-party vendors for online storage of client files was published by the Oregon State Bar Association in 2011. Cloud computing is permissible so long as the attorney “complies with the

duties of competence and confidentiality to reasonably keep the client's information secure" which requires the attorney to take reasonable steps to ensure the vendor will "reliably secure client data and keep information confidential." Attachment P.

### **Pennsylvania**

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility concluded attorneys "may ethically allow client confidential information to be stored in 'the cloud'". An attorney is required to take reasonable care meaning ensuring all materials remain confidential and "reasonable safeguards are employed to ensure that the data is protected". The opinion provides an extensive list of items compromising "reasonable care" for cloud computing, including installing firewalls, avoiding inadvertent disclosure, and verifying the identity of individuals receiving confidential information. Attachment Q.

### **Vermont**

Vermont attorneys are not violating the rules of professional conduct when using a cloud computing service "as long as they take reasonable precautions to protect the confidentiality of and to ensure access to these materials." The opinion relies heavily on previously published opinions from other states. A list of items constituting due diligence is also provided, including a reasonable understanding of the vendor's security system, review of the service provider's security by a technical professional, and being aware of the vendor's commitment to protecting the confidentiality of the data. Attachment R.

### **Virginia**

The Virginia State Bar Association's Legal Ethics Committee concluded cloud computing is permissible if attorneys "act with reasonable care to protect information relating to the representation of a client." Reasonable care requires attorneys to "exercise care in the selection of the vendor", have an expectation that stored data will remain confidential, and specifically instruct the vendor to maintain confidentiality of the data. Attachment S.

### **Washington**

Attorneys in Washington may use cloud computing "as long as the attorney takes reasonable care to ensure that the information will remain confidential and that the information is secure against risk of loss." The advisory opinion provides seven specific "best practices" for evaluating cloud computing services such as evaluating the service provider's "practices, reputation and history" and ensuring the service provider maintains reasonably secure backup measures. Attachment T.

**ATTACHMENT A:**  
**Alabama**

## Opinion Number: 2010-02

---

Retention, Storage, Ownership, Production and Destruction of Client Files  
ETHICS OPINION 2010-02

Retention, Storage, Ownership, Production and Destruction of Client Files

### Introduction

Formal Opinions 1986-02, 1993-10, 1994-01 are the most recent pronouncements of a lawyer's ethical obligations regarding client files. Since those opinions were issued, advances in technology, electronic filing, and internet-based electronic file storage and retrieval services have created issues that were not contemplated by those opinions. Realizing the need to provide guidance to lawyers that is relevant to the practice of law in today's technological world, the Disciplinary Commission offers the following opinion concerning a lawyer's ethical responsibilities relating to the retention, storage, ownership, production and destruction of client files.

### Applicable Rules

The following rules must be considered when determining a lawyer's professional responsibilities relating to client file retention policies. Although most often considered a rule relating solely to lawyer trust accounting, Rule 1.15, Alabama Rules of Professional Conduct, sets out a lawyer's responsibilities relating to types of property of clients or third persons, other than money, and provides, in pertinent part: "(a) A lawyer shall hold the property of clients or third persons that is in the lawyer's possession in connection with a representation separate from the lawyer's own property. [...] Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for six (6) years after termination of the representation...."

"(b) Upon receiving funds or other property in which a client or third person has an interest from a source other than the client or the third person, a lawyer shall promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding that property.

"(c) When in the course of representation a lawyer is in possession of property in which both the lawyer and another person claim interests, the property shall be kept separate by the lawyer until there is an accounting and a severance of their interests. If a dispute arises concerning their respective interests, the portion in dispute shall be kept separate by the lawyer until the dispute is resolved."

\* \* \*

### "COMMENT

"A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property which is the property of clients or third persons should be kept separate from the lawyer's business and personal property and, if monies, in one or more trust accounts...."

\* \* \*

“Third parties, such as a client's creditors, may have just claims against funds or other property in a lawyer's custody. A lawyer may have a duty under applicable law to protect such third-party claims against wrongful interference by the client, and accordingly may refuse to surrender the property to the client. However, a lawyer should not unilaterally assume to arbitrate a dispute between the client and the third party.”

The issue relating to whom the file belongs was decided in Formal Opinion 1986-02, wherein we held that the materials in the file furnished by or for the client are the property of the client. Therefore, Rule 1.15, Ala. R. Prof. C., imposes an ethical and fiduciary duty on the lawyer to properly identify a client's file as such, segregate the file from the lawyer's business and personal property, as well as from the property of other clients and third persons, safeguard and account for its contents, and promptly produce it upon request by the client. Although specifically addressing the issues relating to declining or terminating representation, Rule 1.16(d), Ala. R. Prof. C., also refers to client property and provides, in pertinent part: “(d) Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee that has not been earned. The lawyer may retain papers relating to the client to the extent permitted by other law.”

As we explained in Formal Opinion 1986-02, the file belongs to the client. However, the client's possessory rights to the file are subject to an attorney's lien created by Ala. Code §34-3-61 (1975, as amended), for unpaid fees and expenses. We take this opportunity to reiterate that where a lawyer is asserting a valid attorney's lien pursuant to the Attorney's Lien Statute to secure payment for reasonable fees and expenses that the client has not paid, the lawyer has a statutory right to withhold a client's papers and property in his possession until such time as the client satisfies the lien by tendering payment or makes reasonable and satisfactory arrangements to protect or otherwise secure the lawyer's interest in the unpaid fees and expenses. Rule 1.6, Ala. R. Prof. C., embodies one of the most fundamental principles of our profession and requires that, with few exceptions, a “lawyer shall not reveal information relating to representation of a client.” The duty to maintain confidentiality includes the duty to segregate, protect and safeguard a client's file and the information it contains. The obligation to maintain a client's file contemporaneously organized and orderly filing and indexing system is inherent in the duty of confidentiality and explicit in Rule 1.15. The failure to do so is a breach of Rule 1.15 and may also rise to the level of a breach of Rule 1.6. The principles of confidentiality, loyalty and fidelity are so fundamental to the practice of law that these rules must be enforced to eliminate even the risk of a breach of these principles. However, a lawyer's obligation to identify and segregate a client's file, safeguard its contents, maintain its confidentiality, and promptly account for and produce it upon request from the client, does not create an obligation to preserve permanently all files of the lawyer's clients or former clients. See, D.C. Bar Opinion 206; ABA Informal Op. 1384 (1989). Lawyers do not have unlimited space to store files and what limited space is available is often expensive. Lawyers do have an ethical obligation to prevent the premature or inappropriate destruction of client files. See, D.C. Bar Opinion 205 (1989). Clients may reasonably expect lawyers to maintain valuable and useful information, not otherwise readily available to the client, in their files for a reasonable period of time. ABA Committee on Ethics and Professional Responsibility, Formal Opinion 13384 (March 14, 1977). Adopt File Retention Policies The best practice is for a lawyer to adopt and follow a file retention policy that best fits the needs of the lawyer's practice and the lawyer's clients. File retention policies may vary from lawyer to lawyer and even from client to client, but they must be consistent with the guidelines expressed in this opinion. Additionally, the policy must be communicated to the client in writing at the outset of the representation. Upon conclusion of the representation, the lawyer should reiterate the policy and engage in appropriate follow up with the client regarding retention and destruction of the client's file. The lawyer's file retention policy may be included in the retainer or engagement agreement. In certain situations, it may be necessary and appropriate for a lawyer to create a separate file retention and destruction policy, tailored to meet the specific needs of a client or a client matter, or the lawyer's practice. In developing a file retention and destruction policy, the lawyer must abide by the guidelines expressed in this opinion and should also consider the individual

client's level of education, sophistication, resources and other relevant circumstances. Although as a general rule the file belongs to the client and must be produced promptly upon request, circumstances may exist that would make production of a copy of the entire client's file inappropriate. Absent a court order, a lawyer should not tender the entire file to a client, who has diminished capacity or serious mental health disorders, or to juvenile clients or to clients who have a propensity for violence. A lawyer may also refuse to tender the entire client file to clients who are violent criminal defendants, sex-offenders, or other clients where the information contained in the file would endanger the safety and welfare of the client or others. In these circumstances, it is reasonable and appropriate for the lawyer to redact or remove documents containing sensitive mental health or medical records, descriptions of crimes, photographs of crime scenes or victims, sensitive or salacious information, and personal or other identifying information relating to jurors, victims, witnesses or others. A lawyer's retention and destruction policy should allow for these exceptional situations. How long must a file be retained? Generally, a lawyer should maintain a copy of the client's file for a minimum of six (6) years from termination of the representation or conclusion of the matter. A lawyer's failure to maintain a file for this minimum period of time is presumptively unreasonable based upon consideration of the statute of limitations under the Alabama Legal Services Liability Act (Ala. Code §6-6-574) and the six-year period of limitations for the filing of formal charges in lawyer disciplinary matters (Rule 31, Alabama Rules of Disciplinary Procedure). Six (6) years is the absolute minimum period, but special circumstances may exist that require a longer, even indefinite, period of retention. Files relating to minors, probate matters, estate planning, tax, criminal law, business entities and transactional matters should be retained indefinitely and until their contents are substantively and practically obsolete and their retention would serve no useful purpose to the client, the lawyer, or the administration of justice. What is considered part of the client's file? In general, there are two approaches to determine what constitutes the client's file. The "entire file" approach provides that the client owns and is, therefore, entitled to all of the documents within the client's file, unless the lawyer establishes that withholding items would not result in foreseeable prejudice to the client or would, as previously discussed, endanger the health, safety or welfare of the client or others. In the Matter of Sage Realty Corp. v. Proskauer, Rose, Goetz & Mendelsohn LLP., 91 N.Y. 2d 30, 666 N.Y.S. 2d 985, 689 N.E. 2d 879, 883 (1997); Clark v. Milam, 847 F. Supp. 424, 426 (D. W.Va. 1994); Gottlieb v. Wiles, 143 F.R.D. 241, 247 (D. Colo. 1992); Martin v. Valley Nat. Bank of Arizona, 140 F.R.D. 291 (S.D.N.Y. 1991); Resolution Trust Corp. v. H--, P.C., 128 F.R.D. 647 (N.D. Tex. 1989). The "end product" approach divides ownership of documents in the file between the client and the lawyer and permits a lawyer to retain certain documents, such as notes by the lawyer to himself made in preparation for deposition, trials, or interviews or blemished drafts of other documents, which may contain the lawyer's mental impressions, opinions, and legal theories, some of which may not be flattering or palatable to the client or the lawyer. Corrigan v. Armstrong, Teasdale, Schlafly, Davis & Dicus, et al., 824 S.W.2d 92 (Mo. App. E.D. 1992); Minnesota Lawyers Professional Responsibility Board Opinion 13 (June 15, 1989); ABA Informal Ethics Op. 1376 (Feb. 18, 1977). Either approach requires weighing the protections of both a lawyer's right to think and practice freely during the representation and the client's right to demand an accounting of the actions of his lawyer. The rationale supporting the "end product" approach is that unless the lawyer's recorded thoughts are protected, he will not provide effective representation. The "entire file" approach, which is the majority view, fosters open and forthright lawyer-client relations. The rationale supporting this approach is that a lawyer's fiduciary relationship with a client requires full, candid disclosure. The relationship would be impaired if lawyers withheld any and all documents from their clients without good cause. Henry v. Swift, Currie, McGhee & Hiers, LLP, et al., 581 S.E.2d 37 (Ga. 2003) (Adopting the majority view.) The Disciplinary Commission agrees with the majority of jurisdictions that the "entire file" approach is the best approach. The lawyer is in possession of the file, knows its contents, and is best able to determine the appropriateness of redaction or removal of some of its contents. In those situations where the lawyer determines that production of the entire file is unreasonable or inappropriate, the lawyer must provide reasonable notice to the client that portions of the file have been redacted or items removed for good cause. What contents of a client's file may be destroyed? We have consistently opined that six (6) years is the minimum period of time a lawyer must retain a client's file after the file is closed or after final disposition of the matter. See, Formal Opinions 1994-91 and 1993-10. Although we have opined that six (6) years was generally a reasonable minimum period of time, we are aware that most have assumed that the six (6) year minimum period of time applied to all client files. Today, we emphasize that six (6) years is the minimum period of time that a client's file must be retained, but circumstances may extend that

minimum period of time indefinitely. Even when the passage of time and other circumstances render destruction of a client's file appropriate, there are some contents that should never be destroyed. In Formal Opinion 1993-10, we described the nature of documents that might be contained in a client's file and opined that it was the nature of those documents that determined whether they could be destroyed. We stated that those documents fall into four (4) basic categories. Today, we modify that categorization to simplify the analysis; the results are unchanged. Category 1 property is "intrinsically valuable property." Its "value" is inherent in its nature. Value is not dependent upon certainty of ownership or its source. The fact that the property may be a copy or duplicate, rather than an original, may minimize its value, but this factor, without more, does not change its character as a Category 1 documents. Copies of Category 1 documents must be retained indefinitely, unless the lawyer determines that the copy can be lawfully destroyed because it has been rendered useless and of no value by the client's possession of the original, or by the proper recording of the original, or at the specific written instruction of the client, under circumstances where destruction of the property would not otherwise be illegal or improper. However, the best practice is that the lawyer should never destroy originals of Category 1 property. Where destruction is necessary and appropriate, the lawyer should deliver the original to the client or deposit it with the court. Examples of such property include, but are not limited to: wills, powers of attorney, advance healthcare directives, other executed estate planning documents, stock certificates, bonds, cash, negotiable instruments, certificates of title, abstracts of title, deeds, official corporate or other business and financial records, and settlement agreements. Category 2 property is "valuable property." Its value is dependent upon the present circumstances or upon the reasonably foreseeable probability of a change in future circumstances. Factors that the lawyer may consider are certainty and identity of ownership, source of the property, its intended purpose, its planned or possible use, its character as an original or copy, its form and size, the practicality of preserving or storing it, and the reasonable expectations of the client or owner regarding its ultimate disposition. Category 2 property may be destroyed with the actual consent of the client or upon the client's implied consent, which may be obtained by the client's failure to take possession of the property on or within 60 days of a date established by the lawyer's written file retention policy or as provided in a separate written notice, sent to the client's last known address, advising of the date of the lawyer's planned destruction or disposal of the property. Notice provided as part of the lawyer's written file retention policy, which is affirmatively acknowledged in writing at the outset of the representation or upon termination of the representation, is presumed sufficient and no further notice or attempted notice is required prior to destruction or final disposition of the property. Examples of Category 2 property include, but are not limited to: tangible personal property, photographs, audio and video recordings, pleadings, correspondence, discovery, demonstrative aids, written statements, notes, memoranda, voluminous financial, accounting, or business records, and any other property, the premature or unauthorized destruction of which would be detrimental to the client's present or reasonably foreseeable future interests. Category 3 property is property that has no value or reasonably foreseeable future value. It does not fall into either Category 1 or Category 2. It may be destroyed after the minimum required period of time without notice to or authorization by the client. However, the best practice is for the lawyer to use the same notice procedure for Category 3 property as prescribed for Category 2 property. Documents which fall into category 1 should be retained for an indefinite period of time or preferably should be recorded or deposited with a court. Documents falling into categories 2 and 3 should be retained for a reasonable period of time at the end of which reasonable attempts should be made to contact the client and deliver the documents to him. After the minimum retention period of six (6) years, those documents may be appropriately destroyed. There is no longer a category 4 for purposes of the analysis. Before destroying or disposing of any client file, it is the lawyer's responsibility to review and screen the file to ensure that Category 1 property is not being destroyed. The lawyer must maintain an index of all destroyed files, which index must contain information sufficient to identify the client, the nature or subject matter of the representation, the date the file was opened and closed, the court case number associated with the file, a general description of the type of property destroyed, e.g., "Pleadings, Correspondence, Notes, Legal Research, Videotapes, Photographs," a notation that the file was reviewed for Category 1 property, by whom, whether or not such property was contained in the file, and if so, its location or disposition, and the date and method of destruction of the file. What are the ethical considerations relating to electronic files? The practice of law today often requires legal documents and many other components of a client's file to be converted to, created, transmitted, stored, and reproduced electronically. Moving from "the paper chase" to "the paperless office" presents practical concerns.

Converting existing paper files to electronic format is usually accomplished by “scanning” the paper file, which converts it to a format that can be stored, transmitted, and reproduced electronically. When paper files are converted to electronic format, destruction of the paper file is not without limits or conditions. Even after Category 1 documents are scanned and converted to electronic format, the lawyer cannot destroy the paper Category 1 document. After scanning and conversion, Category 2 and 3 documents may be destroyed, but the best practice is to follow the procedure used for ordinary paper documents. Like documents that are converted, documents that are originally created and maintained electronically must be secured and reasonable measures must be in place to protect the confidentiality, security and integrity of the document. The lawyer must ensure that the process is at least as secure as that required for traditional paper files. The lawyer must have reasonable measures in place to protect the integrity and security of the electronic file. This requires the lawyer to ensure that only authorized individuals have access to the electronic files. The lawyer should also take reasonable steps to ensure that the files are secure from outside intrusion. Such steps may include the installation of firewalls and intrusion detection software. Although not required for traditional paper files, a lawyer must “back up” all electronically stored files onto another computer or media that can be accessed to restore data in case the lawyer’s computer crashes, the file is corrupted, or his office is damaged or destroyed. A lawyer may also choose to store or “back-up” client files via a third-party provider or internet-based server, provided that the lawyer exercises reasonable care in doing so. These third-party or internet-based servers may include what is commonly referred to as “cloud computing.” According to a recent ABA Journal article on the subject, “cloud computing” is a “sophisticated form of remote electronic data storage on the internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored ‘in the cloud’ is kept on large servers located elsewhere and maintained by a vendor.” Richard Acello, *Get Your Head in the Cloud*, ABA Journal, April 2010, at 28-29. The obvious advantage to “cloud computing” is the lawyer’s increased access to client data. As long as there is an internet connection available, the lawyer would have the capability of accessing client data whether he was out of the office, out of the state, or even out of the country. In addition, “cloud computing” may also allow clients greater access to their own files over the internet. However, there are also confidentiality issues that arise with the use of “cloud computing.” Client confidences and secrets are no longer under the direct control of the lawyer or his law firm; rather, client data is now in the hands of a third-party that is free to access the data and move it from location to location. Additionally, there is always the possibility that a third party could illegally gain access to the server and confidential client data through the internet. However, such confidentiality concerns have not deterred other states from approving the use of third-party vendors for the storage of client information. In Formal Opinion No. 33, the Nevada State Bar stated that: “[A]n attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney’s direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third party declines to agree to keep the information confidential, then the attorney violates SCR 156 by transmitting the data to the third party. But if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent.”

In approving on-line file storage, the Arizona State Bar noted in Formal Opinion 09-04 that: “[T]echnology advances may make certain protective measures obsolete over time. Therefore, the Committee does not suggest that the protective measures at issue in Ethics Op. 05-04 or in this opinion necessarily satisfy ER 1.6’s requirements indefinitely. Instead, whether a particular system provides reasonable protective measures must be “informed by the technology reasonably available at the time to secure data against unintentional disclosure.” N.J. Ethics Op. 701. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.”

In their opinions, the Bars of Arizona and Nevada recognize that just as with traditional storage and retention of client files, a lawyer cannot guarantee that client confidentiality will never be breached, whether by an employee or some other third-party. Rather, both Arizona and Nevada adopt the approach that a lawyer only has a duty of reasonable care in selecting and entrusting the storage of confidential client data to a third-party vendor. The Disciplinary Commission agrees and has determined that a lawyer

may use “cloud computing” or third-party providers to store client data provided that the attorney exercises reasonable care in doing so. The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider. In whatever format the lawyer chooses to store client documents, the format must allow the lawyer to reproduce the documents in their original paper format. If a lawyer electronically stores a client’s file and the client later requests a copy of the file, the lawyer must abide by the client’s decision in whether to produce the file in its electronic format, such as on a compact disc or in its original paper format. When a lawyer discards laptops, computers, or other electronic devices, he must take adequate reasonable measures to ensure that client files and/or confidential information have been erased from those items. Failure to do so could result in the disclosure of confidential information to a subsequent user. If such disclosure occurs, the lawyer could be subject to disciplinary action for a violation of Rule 1.6 of the Alabama Rules of Professional Conduct. In what format must the client’s file be delivered? There are various possible combinations of client file formats, including original paper files scanned and converted to electronic document format, original e-documents, and e-mails. Often client files are maintained in part in paper format and electronic format. Rarely is it possible to originate and maintain a client file in electronic format. Therefore, the best practice is to develop a procedure that integrates the various file formats into an organized, indexed and searchable, unified system, so that prompt access to and production of the complete file, regardless of its various formats, can be reasonably assured. Where a client has requested a copy of his file, the file may be produced in the format in which it is maintained by the lawyer, unless otherwise agreed upon or requested by the client. If the client requests that the electronic documents be produced in paper format, then the lawyer must accommodate the client, unless the lawyer’s written file retention policy agreed to by the client provides otherwise. Even in cases where the lawyer’s file retention policy provides that the file will be produced in only electronic format, where the client’s level of education, sophistication, or technological ability, or lack of financial resources, or the unavailability of computer hardware or software necessary to access the documents would create an burden on the client to access the file in electronic format, the lawyer must produce a copy of the file in traditional paper format. Likewise, if the client requests the lawyer to produce the file in electronic format, but the lawyer maintains portions of the file in traditional paper format, the lawyer is not required to produce the file in electronic format, but may simply produce the file in the format in which it is maintained. Can the lawyer charge the client for the cost of copying the file? A lawyer may not charge the client for the cost of providing an initial copy of the file to the client. We note that many lawyers furnish courtesy copies of documents to their clients during the representation. Again, unless the lawyer includes a provision providing otherwise in his written file retention policy, acknowledged by the client at the outset of the representation, providing contemporaneous courtesy copies does not change the lawyer’s obligation to tender the entire file to the client at the termination of the representation. And, the lawyer may not charge the client for copying the entire file, even though courtesy copies of some documents have been previously provided to the client. Although some of the documents being provided to the client may be duplicates, tendering the entire file protects the interests of the client and the lawyer with the assurance that nothing has been overlooked. If the lawyer includes a contrary provision in the client contract or engagement letter which provides that contemporaneous courtesy copies of documents during the representation satisfies his obligation to produce the client’s file, such provision must describe with specificity what documents will be contemporaneously produced, what documents will not be contemporaneously produced, and what procedure and safeguards will be in place to ensure that the contemporaneous courtesy copy policy will be consistently followed. In any case, the client has a right to inspect the lawyer’s file to ensure that the client’s contemporaneous courtesy copy corresponds to the lawyer’s copy of the file. Lawyers may not charge the client for any costs incurred in producing and tendering the file to the client. However, the lawyer may charge reasonable copying costs if a client requests additional copies of his file. As a general rule, the client is responsible to make arrangements to pick up a copy of his file at the lawyer’s place of business. The lawyer may insist on a written acknowledgement of receipt from the client as a condition of surrender of the file. In the event the client refuses to acknowledge receipt of the file, the lawyer may

refuse to tender the file. If the client requests that the file be produced to his authorized agent, then the lawyer should insist on written authorization to do so and should expressly warn the client that production of the file to a third party may defeat confidentiality and attorney-client privilege. Finally, if the client requests that the file be produced by mail, common carrier, or at a location other than the lawyer's office, the client is responsible for the costs associated with such production and the lawyer may withhold production until the client pre-pays the estimated costs or makes arrangements agreeable to the lawyer.

**ATTACHMENT B:**  
**Arizona 2005**

# State Bar of Arizona Ethics Opinions

## **05-04: Electronic Storage; Confidentiality**

7/2005

---

ER's 1.6 and 1.1 require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client's electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end. An attorney who lacks or cannot reasonably obtain that competence is ethically required to retain an expert consultant who does have such competence.

### **FACTS[1]**

The Inquiring Attorney has sought guidance from the Committee regarding the steps the lawyer's firm must take to safeguard electronic client information from Internet hacking and viruses. The Inquiring Attorney's firm has, until recently, kept documents which include confidential client information in electronic form on a computer system which is accessible only from computers within the law firm itself. Although the law firm had access to the internet, that access was through a separate computer system. Neither the computer system on which the client information was stored nor any computer which could access that information was ever connected to the internet.

The Inquiring Attorney's firm now wishes to change that system and allow attorneys and staff to access the internet through the same computers they use to access the client information. Though the Inquiring Attorney does not specifically state this, it is assumed that firm attorneys and other employees will be able to access the client documents remotely. That is, an attorney or other employee may access this information from a computer outside the physical offices of the firm. Such access would be through the internet.

### **QUESTION PRESENTED**

How do we protect the confidentiality and integrity of client information while continuing to increase reliance on internet for research, filings, communication, and storage of documents?

### **RELEVANT ETHICAL RULES**

**ER 1.1 Competence:**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

**ER 1.6(a) Confidentiality of Information:**

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted or required by paragraphs (b), (c), or (d), or ER 3.3(a)(3).

**ER 5.1(a) Responsibilities of Partners, Managers, and Supervisory Lawyers:**

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

**ER 5.3(a) and (b) Responsibilities Regarding Nonlawyer Assistants:**

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; . . .

**OPINION**

It is clear that a lawyer has an ethical obligation to protect the confidences entrusted by clients. Comment 19 to ER 1.6 makes this plain:

[19] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See ERs 1.1, 5.1 and 5.3.

Thus, the short answer to the Inquiring Attorney's inquiry is that a lawyer must act in a competent and reasonable manner to assure that the information in the firm's computer system is not disclosed through inadvertence or unauthorized action. Of course, this syllogism does not really answer the question.

The State Bar of Arizona's Committee on the Rules of Professional Conduct (the "Committee") has not directly addressed this issue. However, in 1997, the Committee addressed the related question of whether an attorney may ethically communicate with clients via e-mail regarding confidential matters. There, the Committee stated that a lawyer may communicate with clients via e-mail. Op. 97-04 (April 7, 1997). However, the Committee warned that a lawyer may want to encrypt the e-mail or use passwords or other electronic measures to guard against inadvertent disclosure. The Committee noted that some courts have deemed e-mail not to be a "sealed" mode of transmission and, thus, subject to unauthorized interception. See, e.g., *American Civil Liberties Union v. Reno*, 929 F.Supp. 824, 834 (E.D.Pa. 1996). The Committee also noted that this recommendation was consistent with the Committee's prior ruling in Op. 95-11 where lawyers were cautioned against discussing "sensitive information" via cellular telephone because of concerns that such discussion may be intercepted. Importantly, the Committee noted that unauthorized interception of cellular telephone calls would be illegal - presumably violating a host of Arizona and Federal laws regarding wire-tapping.

In neither opinion did the Committee deem that the conduct in question was unethical, only that a lawyer should be cautious and take necessary precautions to safeguard client information.

The same reasoning can and should be applied to the questions posed by the Inquiring Attorney. However, it is also important to note that both the law and the practice have changed markedly since 1997. Obviously, the use of e-mail and cellular telephones has significantly expanded since 1997. Moreover, the use of the internet in businesses of all kinds - including the practice of law - has exploded. Not only do more lawyers now use computers than ever before, they use them in ways not imagined ten years ago. It is common to do legal research through the internet - indeed many law firms are abandoning most, if not all, of their physical libraries in favor of on-line resources. It is common for attorneys to exchange correspondence, documents and other information via e-mail and other electronic modes of communication which utilize the internet. Electronic filing in bankruptcy court, for example, requires an internet connection.

Areas of the law relating to client confidences have also changed in recent years. The recent evolution of the law relating to waiver of the attorney-client and work product privileges is instructive. While a lawyer's ethical obligations to safeguard the client's confidences go beyond just protecting privileged material, the reasoning of courts addressing these provisions is most helpful in setting a minimum level of conduct.

The Inquiring Attorney's concerns focuses on what a lawyer must do to protect electronic files from being (1) stolen, (2) inadvertently disclosed to others, and (3) lost or destroyed. All of those scenarios have been extensively discussed by the courts in the context of waiver of the attorney-client or work product privilege.

#### *Stolen Electronic Information - the Purloined Letter.*

The Inquiring Attorney's first concern was that electronic information stored on computers which are also used to access the internet may be subject to "hackers" who wish to steal the client's information. It does not matter whether the hacker's motive is to obtain information for sale or for the hacker's own mysteriously prurient interests.

The courts' treatment of document theft have changed in recent years. Until the late twentieth century, the common rule was that any document, otherwise protected from disclosure by the attorney-client or work product privilege, would lose that privilege if it was disclosed even when such disclosure was caused by theft. This rule, sometimes referred to by commentators as the "Wigmore Rule," has been largely abandoned.

In *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254 (N.D.Ill. 1981), the District Court for the Northern District of Illinois addressed the Wigmore rule and noted the modern trend away from that rule. There, plaintiff routinely searched the trash dumpster located in the parking lot behind the defendant's offices. In the course of these searches, plaintiff discovered drafts of letters and other information which was clearly protected by the attorney-client privilege. Defendants sought to have such documents returned and to prohibit use of those documents at trial.

The court noted that the rule adopted by Wigmore was simple and precise.

. . . [T]he traditional rule effectively presumed that if the parties to a communication intended it to be and remain confidential, they could protect its confidentiality. Accordingly, even where the eavesdropper acted surreptitiously or the communication was stolen, and the parties reasonably expected that it was confidential, the privilege was considered destroyed.

91 FRD at 258 n.3.

However, the court also noted that the modern rule was less draconian and was based upon the notes of the Advisory Commission to Proposed Rule 503, Federal Rules of Evidence. The Commission noted:

. . . Unless intent to disclose [an otherwise privileged communication] is apparent, the attorney-client communication is confidential. Taking or failing to take precautions may be considered as bearing on intent. . . . Substantial authority has in the past allowed the eavesdropper to testify to overheard privileged conversations and has admitted intercepted privileged letters. Today, the evolution of more sophisticated techniques of eavesdropping and interception calls for abandonment of this position. The [proposed] rule accordingly adopts a policy of protection against these kinds of invasion of the privilege.

91 F.R.D. at 260 n. 4.

However, this "modern rule" does not wholly relieve the attorney or his client from taking precautions against theft and disclosure. The court held that preservation of the privilege does not "in any way reduce the client's need to take all possible precautions to insure confidentiality." 91 F.R.D. at 260 (quoting 2 *Weinstein's Evidence*, 503(b)(2)).

Thus, the modern rule is that precautions must be taken to prevent the theft of confidential communications to preserve the privilege.

*Inadvertent Disclosure*

Instances where privileged information has been stolen are relative rare. More common is the predicament where a lawyer has inadvertently disclosed otherwise privileged information. The Eighth Circuit Court of Appeals has summarized the three approaches generally taken in analyzing the effect of inadvertent disclosure. First, it notes what it refers to as the "lenient" approach.

Under the lenient approach, attorney-client privilege must be knowingly waived. Here the determination of inadvertence is the end of the analysis. The attorney-client privilege exists for the benefit of the client and cannot be waived except by an intentional and knowing relinquishment.

*Gray v. Bicknell*, 86 F.3d 1472, 1483 (8th Cir. 1996) (citing cases from the Southern District of Florida and the Northern District of Illinois).

The Eighth Circuit rejected that rule. A privileged document must be confidential to retain its privilege but, the court stated, "under this test, the lack of confidentiality becomes meaningless. . ." *Id.*

The court also rejected what it called the "strict" test.

. . . Under the strict test, any document produced, either intentionally or otherwise, loses its privileged status with the possible exception of situations where all precautions were taken. Once waiver has occurred, it extends "to all other communications relating to the same subject matter."

*Id.* at 1483 (citing cases from the DC and First Circuits).

Noting that the strict test has "some appeal" because it makes attorneys and clients accountable for their own carelessness, the Eighth Circuit rejected it "because of its pronounced lack of flexibility and its significant intrusion on the attorney-client relationship." *Id.*

Ultimately, the Eighth Circuit adopted what it called the "middle-of-the-road" test, sometimes referred to as the "Hydraflow test" after *Hydraflow, Inc. v. Enidine, Inc.*, 145 F.R.D. 626 (WDNY 1993). This test sets out a five-part analysis to determine whether inadvertently disclosed documents retain their privileged status.

. . . These considerations are: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of document production, (2) the number of inadvertent disclosures, (3) the extent of the disclosures, (4) the promptness of measures taken to rectify the disclosure, and (5) whether the overriding interest of justice would be served by relieving the party of its error.

*Id.* at 1483-84.

While no Arizona State court has directly addressed these issues, the Arizona Federal District Court has. In *Resolution Trust Corporation v. Dean*, 813 F.Supp. 1426 (D. Ariz. 1993), a senior

attorney representing the Resolution Trust Corporation ("RTC") prepared an internal memorandum discussing the RTC's investigation of certain claims it was pursuing against J. Fife Symington relating to the Camelback Esplanade project in Phoenix, Arizona. The memorandum (called the "ATS Memo") discussed possible claims against Symington, possible defenses to such claims, the probability of success on those claims and defenses, the cost of proceeding and the likelihood of recovery. The ATS Memo was deemed by the court to be covered by the attorney-client privilege.

Unfortunately, all or part of the ATS Memo was "leaked" to the press. Defendants sought production of the entire document, the RTC refused, and a motion to compel production followed. The court's analysis followed and expressly relied upon two different cases, *In re Grand Jury Proceedings Involving Berkley & Co.*, 466 F.Supp. 863 (D. Minn. 1979) ("Berkley") and *In re Dayco Corp. Derivative Securities Litigation*, 102 F.R.D. 468 (S.D. Ohio 1984) ("Dayco"). The RTC claimed that, because it had taken extensive precautions against disclosure of the ATS Memo and because it could not determine how the document was leaked to the press, such disclosure was unauthorized and amounted to a crime.

The Arizona District Court noted that, in *Berkley*, the Minnesota Court held that, "to the extent the documents can be viewed as stolen, they should not lose the protection of the attorney-client privilege." *RTC v. Dean*, at 1429. It also noted that, before reaching that conclusion, the Minnesota Court conducted an in camera review of the documents to determine the privilege status and ordered Berkley to "provide information as to the manner in which it maintains its records." *Id.*

Defendants argued that, unlike the situation in *Berkley*, there was no evidence that the ATS Memo had been stolen. The Arizona court found this distinction to be without merit, stating:

. . . This argument rests on a narrow reading of *Berkley*, for although there is no evidence of thievery in this case at bar, there is an indication that the disclosure of the documents was in itself a criminal act.

*Id.*

The Arizona court then turned to the *Dayco* case. There, although the subject documents were also leaked to the press, the documents were not prepared by the government and, thus, such action did not amount to a crime. The Arizona court noted with approval that the *Dayco* court first examined the documents and the manner in which they were kept before reaching its holding:

. . . The [*Dayco*] court held that, absent any indication that the defendants voluntarily gave the diary to the press, publication of excerpts of the diary should not be considered a waiver of the privilege. *Id.* citing J. Weinstein & M. Berger, *Weinstein's Evidence*, para 503(a)(4)[01] at 503-31 (1982 ed.) ("**Communications which were intended to be confidential but are intercepted despite reasonable precautions remain privileged.**")

*Id.* (emphasis added).

In the end, the Arizona court found that the facts before it to be "roughly analogous to those in *Berkley* and *Dayco*." The court held that, despite the disclosure of the ATS Memo to the press, the document retained its privileged status because the RTC had affirmatively demonstrated that it had taken "precautions to secure the confidentiality of the ATS memo and that the memo's leak remains inexplicable." *Id.* at 1429-30.

ER 1.6 requires a lawyer to take reasonable precautions to protect client confidences. The foregoing analysis outlines the kind of procedures the courts have followed in the similar situation of determining when an otherwise privileged communication loses its privileged status because of involuntary disclosure.

It is not difficult, in that light, to conclude that an attorney must take similar precautions with regard to electronically stored communications. It is plain that some efforts must be undertaken. A panoply of electronic and other measures are available to assist an attorney in maintaining client confidences. "Firewalls" - electronic devices and programs which prevent unauthorized entry into a computer system from outside that system - are readily available. Recent upgrades in Microsoft operating systems incorporate such software systems automatically. A host of companies, including Microsoft, Symantec, McAfee and many others, provide security software that helps prevent both destructive intrusions (such as viruses and "worms") and the more malicious intrusions which allow outsiders access to computer files (sometimes call "adware" or "spyware").

Software systems are also readily available to protect individual electronic files. Passwords can be added to files which prevent viewing of such files unless a password is first known and entered. The files themselves can also be encrypted so that, even if the password protection is compromised, the file cannot be read without knowing the encryption key - something that is extremely difficult to break.

Precisely which of these software and hardware systems should be chosen - and the extent to which they must be employed - is beyond the scope and competence of the Committee. This is the kind of thing each attorney must assess. The expectation of the client that the client's records and communications will be held in confidence is significant.

As set forth in the Comment to ER 1.6, an attorney must not only take reasonable precautions to protect client confidences, the lawyer must "act competently" in that regard. ER 1.1 requires, in general terms, that a lawyer act competently with regard to client representation. ER 5.1 and 5.3 require that a lawyer manage the lawyer's firm and assistants in such a way as to be certain that the lawyer's ethical responsibilities are discharged. Once again, it is the lawyer's individual responsibility to know when the lawyer can act competently or not.

It is not surprising that few lawyers have the training or experience required to act competently with regard to computer security. Such competence is, however, readily available. Much information can be obtained through the internet by an attorney with sufficient time and energy to research and understand these systems. Alternatively, experts are readily available to assist an attorney in setting up the firm's computer systems to protect against theft of information and inadvertent disclosure of client confidences.

Malicious Destruction of Client Files

The Inquiring Attorney also expressed concern that allowing access to client files on computers which are also used to access the internet can lead to the malicious destruction of those files. The threat of such destructive viruses is well known.

As with the inadvertent disclosure analysis above, ER 1.6 and 1.1 require the lawyer to act competently in assuring that electronic information transmitted to the attorney is not lost or destroyed. Much of the security software and hardware discussed above provides protection against such destructive intrusions. Moreover, it is common practice to routinely back-up computer files. In that way, even if a computer system is entirely disabled through malicious attack, nearly all data can be retrieved from back-up files. Easy to use and inexpensive systems are available to make this kind of back-up an automatic process.

Once again, the extent to which such systems need to be employed and which systems best accomplish that goal is something which an individual attorney must determine. Doing so competently may require additional research or the employment of an expert consultant.

**CONCLUSION**

ER's 1.6 and 1.1 require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client's electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.

---

[1] Formal Opinions of the Committee on the Rules of Professional Conduct are advisory in nature only and are not binding in any disciplinary or other legal proceedings. © State Bar of Arizona 2003

**ATTACHMENT C:**  
**Arizona 2009**

# State Bar of Arizona Ethics Opinions

**09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet**  
12/2009

---

Lawyers providing an online file storage and retrieval system for client access of documents must take reasonable precautions to protect the security and confidentiality of client documents and information. Lawyers should be aware of limitations in their competence regarding online security measures and take appropriate actions to ensure that a competent review of the proposed security measures is conducted. As technology advances over time, a periodic review of the reasonability of security precautions may be necessary.

## **FACTS**

The inquiring lawyer wants to offer a service to clients that would allow clients online access to view and retrieve client files. The lawyer designed a multi-level security system in an effort to maintain the confidentiality and security of the files. First, the client files would be accessible only through a Secure Socket Layer (SSL) server, which encodes documents, making it difficult for third parties to intercept or read them. Second, the lawyer would assign unique randomly generated alpha-numeric names and passwords to each online client folder. The folder names contain no information that could identify the client to which it belongs. The password would not be the same as the client folder name. Third, all online client files would be converted to Adobe PDF (Portable Document Format) files and protected with another randomly generated unique alpha-numeric password.

## **QUESTION PRESENTED**

May the inquiring lawyer maintain an encrypted online file storage and retrieval system for clients in which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alpha-numeric names and passwords?

## **APPLICABLE ARIZONA RULES OF PROFESSIONAL CONDUCT (“ER \_\_”)**

### **ER 1.1 Competence**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

### **ER 1.6 Confidentiality of Information**

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted or required by paragraphs (b), (c) or (d) or ER 3.3(a)(3).

....

## RELEVANT ARIZONA ETHICS OPINIONS

Ariz. Ethics Ops. [05-04](#), [07-02](#)

### OPINION

This Committee has already determined that electronic storage of client files is permissible as long as lawyers and law firms “take competent and reasonable steps to assure that the client’s confidences are not disclosed to third parties through theft or inadvertence.” Ethics Op. 05-04. In that opinion, the Committee analyzed the ethical implications of storing client information electronically on systems accessible through the Internet. Then, as today, the primarily applicable rule is ER 1.6. Comment 19 to ER 1.6 states:

A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.

Thus, it is clear “that a lawyer must act in a competent and reasonable manner to assure that the information in the firm’s computer system is not disclosed through inadvertence or unauthorized action.” Ethics Op. 05-04. After analyzing the precautions required by courts to safeguard lawyer-client privileged information, we concluded that similar precautions were required for compliance with ER 1.6. *Id.*

The “panoply of electronic and other measures ... available to assist an attorney in maintaining client confidences” remains similar to those discussed in Ethics Op. 05-04. In satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc. *Id.* Indeed, these considerations have become more relevant as more law offices and departments convert to “paperless” file storage. *See, e.g.*, Ethics Op. 07-02.

Other bar associations have recognized that the duty to take reasonable precautions does not require a guarantee that the system will be invulnerable to unauthorized access. *See, e.g.*, N.J. Ethics Op. 701 (Apr. 10, 2006). Instead, the lawyer “is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access.” *Id.* *See also* 2008 N.C. Formal Ethics Op. 5 (“law firm must enact appropriate measures to ensure that each client only has access to his or her own file [and] that third parties cannot gain access [to] any client file”).

It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field. The competence requirements of ER 1.1 apply not only to a lawyer’s legal skills, but also generally to “those matters reasonably necessary for the representation.” Therefore, as a necessary prerequisite to making a determination regarding the

reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security.

Based on the facts supplied by the inquiring lawyer, the proposed online client file system appears to meet the requirements set forth by ER 1.6 and interpreted in Ethics Op. 05-04. [1] The lawyer has taken the preliminary step of having the files protected by a Secure Socket Layer (SSL) server, which encrypts the files, and also applied several layers of password protection. The fact that the system also utilizes unique and randomly generated folder names and passwords appears to satisfy the requirement of taking reasonable measures to protect client confidentiality and prevent unauthorized access. The further measure of converting each document to PDF format and requiring another unique alpha-numeric password to review its contents enhances the security of the proposed system.

However, the Committee also recognizes that technology advances may make certain protective measures obsolete over time. Therefore, the Committee does not suggest that the protective measures at issue in Ethics Op. 05-04 or in this opinion necessarily satisfy ER 1.6's requirements indefinitely. Instead, whether a particular system provides reasonable protective measures must be "informed by the technology reasonably available at the time to secure data against unintentional disclosure." N.J. Ethics Op. 701. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information.

## CONCLUSION

The inquiring lawyer appears to have satisfied the obligation to take reasonable precautions to protect the security and confidentiality of client documents and information. The proposed system uses encryption and three layers of unique randomly generated alpha-numeric folder names and passwords. Although the proposed system appears to constitute a reasonable precaution at this time, competent personnel should conduct periodic reviews to ensure that security precautions in place remain reasonable as technology progresses.

**Formal opinions of the Committee on the Rules of Professional Conduct are advisory in nature only and are not binding in any disciplinary or other legal proceedings. This opinion is based on the Ethical Rules in effect on the date the opinion was published. If the rule changes, a different conclusion may be appropriate. © State Bar of Arizona 2009**

---

[1] In so concluding, the Committee does not intend to suggest that all of the measures employed by the inquiring lawyer are necessary to comply with ER 1.6.

**ATTACHMENT D:**  
**California**

**THE STATE BAR OF CALIFORNIA  
STANDING COMMITTEE ON  
PROFESSIONAL RESPONSIBILITY AND CONDUCT  
FORMAL OPINION NO. 2010-179**

**ISSUE:** Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

**DIGEST:** Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

**AUTHORITIES  
INTERPRETED:**

Rules 3-100 and 3-110 of the California Rules of Professional Conduct.

Business and Professions Code section 6068, subdivision (e)(1).

Evidence Code sections 917(a) and 952.

**STATEMENT OF FACTS**

Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm's access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm's computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney's supervisor is also permitted access to Attorney's computer to review the substance of his work and related communications.

Client has asked for Attorney's advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

**DISCUSSION**

Due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law. The Committee's own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology. Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this

opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology.

## **1. The Duty of Confidentiality**

In California, attorneys have an express duty “[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.”<sup>1/</sup> (Bus. & Prof. Code, § 6068, subd. (e)(1).) This duty arises from the relationship of trust between an attorney and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has very few exceptions. (Rules Prof. Conduct, rule 3-100 & discussion “[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law.”)<sup>2/</sup>

Unlike Rule 1.6 of the Model Rules of Professional Conduct (“MRPC”), the exceptions to the duty of confidentiality under rule 3-100 do not expressly include disclosure “impliedly authorized in order to carry out the representation.” (MRPC, Rule 1.6.) Nevertheless, the absence of such language in the California Rules of Professional Conduct does not prohibit an attorney from using postal or courier services, telephone lines, or other modes of communication beyond face-to-face meetings, in order to effectively carry out the representation. There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation,<sup>3/</sup> on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client’s matter,<sup>4/</sup> on the other hand.

Section 952 of the California Evidence Code, defining “confidential communication between client and lawyer” for purposes of application of the attorney-client privilege, includes disclosure of information to third persons “to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted.” (Evid. Code, § 952.) While the duty to protect confidential client information is broader in scope than the attorney-client privilege (Discussion [2] to rule 3-100; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]), the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information. (See Cal. State Bar Formal Opn. No. 2003-161 [repeating the Committee’s prior observation “that the duty of confidentiality and the evidentiary privilege share the same basic policy foundation: to encourage clients to disclose all possibly pertinent information to their attorneys so that the attorneys may effectively represent the clients’ interests.”].) Pertinent here, the manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence, and determining whether a third party has the ability to access and use confidential client information in a manner that is unauthorized by the client is a subject that must be considered in conjunction with that duty.

## **2. The Duty of Competence**

Rule 3-110(A) prohibits the intentional, reckless or repeated failure to perform legal services with competence. Pertinent here, “competence” may apply to an attorney’s diligence and learning with respect to handling matters for clients. (Rules Prof. Conduct, rule 3-110(B).) The duty of competence also applies to an attorney’s “duty to supervise the work of subordinate attorney and non-attorney employees or agents.” (Discussion to rule 3-110.)

---

<sup>1/</sup> “Secrets” include “[a]ny ‘information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.’” (Cal. State Bar Formal Opn. No. 1981-58.)

<sup>2/</sup> Unless otherwise indicated, all future references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

<sup>3/</sup> In this regard, compare Cal. State Bar Formal Opn. No. 1971-25 (use of an outside data processing center without the client’s consent for bookkeeping, billing, accounting and statistical purposes, if such information includes client secrets and confidences, would violate section 6068, subdivision (e)), with Los Angeles County Bar Assn. Formal Opn. No. 374 (1978) (concluding that in most circumstances, if protective conditions are observed, disclosure of client’s secrets and confidences to a central data processor would not violate section 6068(e) and would be the same as disclosures to non-lawyer office employees).

<sup>4/</sup> Cf. Evid. Code, § 917(b) (“A communication . . . does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.”).

With respect to acting competently to preserve confidential client information, the comments to Rule 1.6 of the MRPC<sup>5/</sup> provide:

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

(MRPC, cmts. 16 & 17 to Rule 1.6.) In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections.

### **3. Factors to Consider**

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:<sup>6/</sup>

- a) The attorney's ability to assess the level of security afforded by the technology, including without limitation:
  - i) Consideration of how the particular technology differs from other media use. For example, while one court has stated that, "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)" (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 834, aff'd (1997) 521 U.S. 844 [117 S.Ct. 2329]), most bar associations have taken the position that the risks of a third party's unauthorized review of email (whether by interception or delivery to an unintended recipient) are similar to the risks that confidential client information transmitted by standard mail service will be opened by any of the many hands it passes through on the way to its recipient or will be misdirected<sup>7/</sup> (see, e.g., ABA Formal Opn. No. 99-413<sup>8/</sup> [concluding that attorneys have a reasonable expectation of privacy in email communications, even if unencrypted, "despite some risk of interception and disclosure"]; Los Angeles County Bar Assn. Formal Opn. No. 514 (2005) ["Lawyers are not required

---

<sup>5/</sup> In the absence of on-point California authority and conflicting state public policy, the MRPC may serve as guidelines. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771].)

<sup>6/</sup> These factors should be considered regardless of whether the attorney practices in a law firm, a governmental agency, a non-profit organization, a company, as a sole practitioner or otherwise.

<sup>7/</sup> Rule 1-100(A) provides that "[e]thics opinions and rules and standards promulgated by other jurisdictions and bar associations may . . . be considered" for professional conduct guidance.

<sup>8/</sup> In 1999, the ABA Committee on Ethics and Professional Responsibility reviewed state bar ethics opinions across the country and determined that, as attorneys' understanding of technology has improved, the opinions generally have transitioned from concluding that use of Internet email violates confidentiality obligations to concluding that use of unencrypted Internet email is permitted without express client consent. (ABA Formal Opn. No. 99-413 [detailing various positions taken in state ethics opinions from Alaska, Washington D.C., Kentucky, New York, Illinois, North Dakota, South Carolina, Vermont, Pennsylvania, Arizona, Iowa and North Carolina].)

to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes.”]; Orange County Bar Assn. Formal Opn. No. 97-0002 [concluding use of encrypted email is encouraged, but not required.] (See also *City of Reno v. Reno Police Protective Assn.* (2003) 118 Nev. 889, 897-898 [59 P.3d 1212] [referencing an earlier version of section 952 of the California Evidence Code and concluding “that a document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met.”].)

- ii) Whether reasonable precautions may be taken when using the technology to increase the level of security.<sup>9/</sup> As with the above-referenced views expressed on email, the fact that opinions differ on whether a particular technology is secure suggests that attorneys should take reasonable steps as a precautionary measure to protect against disclosure.<sup>10/</sup> For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. To place the risks in perspective, it should not be overlooked that the very nature of digital technologies makes it easier for a third party to intercept a much greater amount of confidential information in a much shorter period of time than would be required to transfer the same amount of data in hard copy format. In this regard, if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.<sup>11/</sup> Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended. (See David Ries & Reid Trautz, *Law Practice Today*, “Securing Your Clients’ Data While On the Road,” October 2008 [noting reports that “as many as 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered”].)
- iii) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if a license to use certain software or a technology service imposes a requirement of third party access to information related to the attorney’s use of the technology, the attorney may need to confirm that the terms of the requirement or authorization do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose, particularly if the information at issue is highly sensitive.<sup>12/</sup> “Under Rule 5.3 [of the MRPC], a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that

---

<sup>9/</sup> Attorneys also should employ precautions to protect confidential information when in public, such as ensuring that the person sitting in the adjacent seat on an airplane cannot see the computer screen or moving to a private location before discussing confidential information on a mobile phone.

<sup>10/</sup> Section 60(1)(b) of the Restatement (Third) of The Law Governing Lawyers provides that “a lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer’s associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client.”

<sup>11/</sup> Similarly, this Committee has stated that if an attorney is going to maintain client documents in electronic form, he or she must take reasonable steps to strip any metadata containing confidential information of other clients before turning such materials over to a current or former client or his or her new attorney. (See Cal. State Bar Formal Opn. 2007-174.)

<sup>12/</sup> A similar approach might be appropriate if the attorney is employed by a non-profit or governmental organization where information may be monitored by a person or entity with interests potentially or actually in conflict with the attorney’s client. In such cases, the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent access to confidential client information. The attorney also may need to consider whether he or she can competently represent the client without the technology.

the service provider will not make unauthorized disclosures of client information. Thus when a lawyer considers entering into a relationship with such a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard. [Citation.] In connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality.” (ABA Formal Opn. No. 95-398.)

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.<sup>13/</sup> (Cf. Rules Prof. Conduct, rule 3-110(C) [“If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.”].)

- b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person’s electronic information. The fact that a third party could be subject to criminal charges or civil claims for intercepting, accessing or engaging in unauthorized use of confidential client information favors an expectation of privacy with respect to a particular technology. (See, e.g., 18 U.S.C. § 2510 et seq. [Electronic Communications Privacy Act of 1986]; 18 U.S.C. § 1030 et seq. [Computer Fraud and Abuse Act]; Pen. Code, § 502(c) [making certain unauthorized access to computers, computer systems and computer data a criminal offense]; Cal. Pen. Code, § 629.86 [providing a civil cause of action to “[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of [Chapter 1.4 on Interception of Wire, Electronic Digital Pager, or Electronic Cellular Telephone Communications].”]; *eBay, Inc. v. Bidder’s Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058, 1070 [in case involving use of web crawlers that exceeded plaintiff’s consent, court stated “[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another’s personal property, is sufficient to establish a cause of action for trespass to chattel.”].<sup>14/</sup>)
- c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.<sup>15/</sup> As noted above, if another person may have access to the communications transmitted between the attorney and the client (or others necessary to the representation), and may have an interest in the information being disclosed that is in conflict with the client’s interest, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology. These types of situations increase the likelihood for intrusion.

---

<sup>13/</sup> Some potential security issues may be more apparent than others. For example, users of unsecured public wireless connections may receive a warning when accessing the connection. However, in most instances, users must take affirmative steps to determine whether the technology is secure.

<sup>14/</sup> Attorneys also have corresponding legal and ethical obligations not to invade the confidential and privileged information of others.

<sup>15/</sup> For the client’s consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client’s decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

- d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.<sup>16/</sup> Section 917(a) of the California Evidence Code provides that “a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship ... is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential.” (Evid. Code, § 917(a).) Significantly, subsection (b) of section 917 states that such a communication “does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.” (Evid. Code, § 917(b). See also Penal Code, § 629.80 [“No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of [Chapter 1.4] shall lose its privileged character.”]; 18 U.S.C. § 2517(4) [“No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [18 U.S.C. § 2510 et seq.] shall lose its privileged character.”].) While these provisions seem to provide a certain level of comfort in using technology for such communications, they are not a complete safeguard. For example, it is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver.<sup>17/</sup> Further, the analysis differs with regard to an attorney’s duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.
- e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.
- f) Client instructions and circumstances. If a client has instructed an attorney not to use certain technology due to confidentiality or other concerns or an attorney is aware that others have access to the client’s electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should not be used in the course of the representation.<sup>18/</sup>

#### 4. **Application to Fact Pattern**<sup>19/</sup>

In applying these factors to Attorney’s situation, the Committee does not believe that Attorney would violate his duties of confidentiality or competence to Client by using the laptop computer because access is limited to authorized individuals to perform required tasks. However, Attorney should confirm that personnel have been appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110. (See *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] [“An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority.”]; *In re Complex Asbestos Litig.* (1991) 232 Cal.App.3d 572, 588 [283 Cal.Rptr. 732] [discussing law firm’s ability to supervise employees and ensure they protect client confidences]; Cal. State Bar Formal Opn. No. 1979-50 [discussing lawyer’s duty to explain to

<sup>16/</sup> Consideration of evidentiary issues is beyond the scope of this opinion, which addresses only the ethical implications of using certain technologies.

<sup>17/</sup> For example, with respect to the impact of inadvertent disclosure on the attorney-client privilege or work-product protection, rule 502(b) of the Federal Rules of Evidence states: “When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: 1. the disclosure is inadvertent; 2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and 3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).” As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

<sup>18/</sup> In certain circumstances, it may be appropriate to obtain a client’s informed consent to the use of a particular technology.

<sup>19/</sup> In this opinion, we are applying the factors to the use of computers and wireless connections to assist the reader in understanding how such factors function in practice. Use of other electronic devices would require similar considerations.

employee what obligations exist with respect to confidentiality[.]) In addition, access to the laptop by Attorney's supervisor would be appropriate in light of her duty to supervise Attorney in accordance with rule 3-110 and her own fiduciary duty to Client to keep such information confidential.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.<sup>20/</sup> Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.<sup>21/</sup>

Finally, if Attorney's personal wireless system has been configured with appropriate security features,<sup>22/</sup> the Committee does not believe that Attorney would violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection.

### CONCLUSION

An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

---

<sup>20/</sup> Local security features available for use on individual computers include operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions, while network safeguards that may be employed include network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring. This list is not intended to be exhaustive.

<sup>21/</sup> Due to the possibility that files contained on a computer may be accessed by hackers while the computer is operating on an unsecure network connection and when appropriate local security features, such as firewalls, are not enabled, attorneys should be aware that *any* client's confidential information stored on the computer may be at risk regardless of whether the attorney has the file open at the time.

<sup>22/</sup> Security features available on wireless access points will vary and should be evaluated on an individual basis.

**ATTACHMENT E:**  
**Connecticut**



*Professional Ethics Committee*

30 Bank Street  
PO Box 350  
New Britain  
CT 06050-0350  
06051 for 30 Bank Street  
P: (860) 223-4400  
F: (860) 223-4488

Approved June 19, 2013

**Informal Opinion 2013-07**  
**Cloud Computing**

The question addressed in this Opinion is whether it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law.

Technological change tends to outpace the law. There is a great deal being written about cloud computing every day. This opinion is a starting point for issues raised by a lawyer's use of cloud computing, but the field will continue to develop and due diligence will require a lawyer to keep pace with emerging standards. For the purpose of this opinion, cloud computing includes the storage, transmission, and processing of data (client information) using shared computer facilities owned or leased by a third party service provider. The facilities and services are typically accessed over the internet by means of different networked devices including computers, tablets, laptops, smart phones, and other devices.<sup>1</sup>

In a familiar model, a user may be provided with applications referred to as Software as Service ("SAAS"), that operate on a cloud infrastructure which may be located at remote sites in and outside of Connecticut, including foreign countries. The cloud service provider owns or leases the data processing equipment and the information technology and also manages the system. In the modality which this Opinion addresses – called public cloud computing – the use of the online computer resources is shared with other members of the public.<sup>2</sup> In related activities, a user may entrust data for online storage only (i.e., by using such vendors as are located at mozy.com and cabonite.com) and for online transmission (email via vendors such as aol.com, yahoo.com, gmail.com, outlook.com, etc.). Cloud computing has been the subject of a great deal of commentary; attempts to describe cloud computing have been problematic because cloud computing is not a single kind of system, but instead spans a spectrum of underlying technologies, configuration possibilities, service models, and deployment models.<sup>3</sup>

Cloud computing can provide significant economy and technological benefit for the user compared to what is financially available through the ownership or lease of equipment, direct license of software, and hired information technology personnel. The cloud service providers tend to use a "pay-as-you-go" billing format that offers enormous advantages for users with

---

<sup>1</sup> See National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication #800-145 (September 2011).

<sup>2</sup> Deployment models include private cloud, community cloud, public cloud, and hybrid cloud infrastructures. NIST #800-145.

<sup>3</sup> National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication #800-146 (May 2012) and Special Publication #800-144 (December 2011).

limited or irregular cash flow. With cloud computing, a user has the option to create a virtual office with only limited ownership of data processing, transmission, and data storage equipment.

The ultimate responsibility for insuring the privacy and security of the data resides with the user purchasing the cloud services. While much of the physical, technical, and administrative safeguards are handled by the cloud service provider, the user will still retain responsibility for a significant portion of these safeguards.

Ordinarily the cloud service provider offers an agreement to a user, which may be called Service Level Agreement (“SLA”) or Terms of Service. The terms of such agreements can vary amongst the different service providers, and different terms have different impacts on a lawyer’s obligations under applicable law and Rules of Professional Responsibility; this Opinion is limited to discussion of the Connecticut-licensed lawyer’s obligations under the Connecticut Rules of Professional Responsibility when using cloud computing.

The privilege of practicing law comes with professional obligations and those obligations extend to the use of technology. Rule 1.1 Official Commentary (effective [month, year]) expressly provides that in order “to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . .” Lawyers who use cloud computing have a duty to understand its potential impact on their obligations under applicable law and under the Rules of Professional Responsibility. If a lawyer is unable to meet these obligations when using a given type of technology or service provider, the lawyer should not use the technology or the service provider. In order to determine whether use of a particular technology or hiring a certain particular service provider is consistent or compliant with the lawyer’s professional obligations, a lawyer must engage in due diligence.

Lawyers have professional obligations which include the duty to preserve client information (Rules 1.6 and Rule 1.15) as well as the duty to comply with and respond to legitimate inquiry from disciplinary authorities. Rule 1.15(k) and Practice Book §2-27(c). The issue of how a lawyer stores and processes business records affects the lawyer’s ability to discharge these duties. Modern technologies allow for data to be processed, transmitted, and stored some place other than a lawyer’s workplace. Lawyers’ remote storage of data is not a new phenomenon; lawyers have been using off-site storage providers for many years, and the issues remain the same whether tangible records are stored in a “brick-and-mortar” warehouse or intangible data is stored on third party servers.

Rule 1.6 of the Rules of Professional Conduct governs the confidentiality of client information. In relevant part, Rule 1.6(a) provides that “a lawyer shall not reveal confidential information relating to the representation of a client unless the client consents after consultation . . . .” The duty of confidentiality imposed by Rule 1.6(e) (effective January 1, 2014) requires a lawyer to avoid using means or methods of holding and delivering data that present an unreasonable risk of unintended disclosure to and access by unauthorized third parties. The duty of confidentiality described in Rule 1.6 is rigid but tempered by the recognition that even when a lawyer acts competently to preserve the confidentiality of the data, reasonable safeguards some times fail:

The unauthorized access to, or the inadvertent or unauthorized

disclosure of, information relating to the representation of a client does not constitute a violation of subsection (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Rule 1.6, Official Commentary (effective January 1, 2014).

This Committee previously addressed issues of client confidentiality presented by a lawyer's use of the Internet and remote access capabilities in Informal Opinion 99-52, in which the Committee concluded that a lawyer's use of unencrypted internet email to engage in communication with a client did not violate Rule 1.6(a) in ordinary circumstances. However:

[I]f circumstances exist which would place a lawyer on notice that there is a greater than ordinary risk of interception or unauthorized disclosure (such as an email "mailbox" which is accessible to persons other than the intended recipient), regardless of the relative sophistication of the email recipient, use of email to transmit confidential information without the express authorization and consent of the client would be unwise and unethical.

In a similar fashion, where the information sought to be communicated is of an extraordinary sensitive or highly confidential nature, such that any unauthorized disclosure could cause serious injury to the interests of the client, the lawyer should choose a means of communication that provides a level of security proportional to the heightened need to avoid any threat of disclosure of the information. Because of this, the consent of the client should be obtained before transmitting any email containing information of an extraordinarily sensitive or highly confidential nature, just as a wise and prudent lawyer would obtain the consent of the client before communicating significant, consequential, and extremely sensitive privileged matters through telephone lines, fax machines, or even regular mail.

Informal Opinion 99-52.

While the specific technology examined by the Committee in 1999 (for Informal Opinion 99-52) might now be obsolete, the need for a lawyer to thoughtfully and thoroughly evaluate the risks presented by the use of current technology remains as vital as ever. The Rules permit a lawyer to use the Internet to transmit, store and process data using shared computer facilities from the reasonably reliable cloud service provider as long as the lawyer undertakes reasonable efforts to prevent unauthorized access to or disclosure of such data. As considered by this Committee in 1999, the lawyer's efforts must be commensurate with the risk presented. The lawyer should be satisfied that the cloud service provider's (1) transmission, storage and possession of the data does not diminish the lawyer's ownership of and unfettered accessibility to the data, and (2) security policies and mechanisms to segregate the lawyer's data and prevent unauthorized access to the data by others including the cloud service provider.<sup>4</sup>

The lawyer's obligations regarding the security for such data are not independent from but consistent with Rule 1.15, which requires that property of clients and third persons which the lawyer receives should be "appropriately safeguarded." Client property in the context of Rule 1.15 generally includes files, information and documents including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

(b) A lawyer shall hold property of clients and third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . . Other property shall be identified as such and appropriately safeguarded.

Further, the lawyer using cloud computing must ensure the service provider's conduct is compatible with the professional obligations of the lawyer. Rule 5.3 addresses the lawyer's responsibilities regarding nonlawyer assistants and states:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (1) A partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.
- (2) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
- (3) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: (A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (B) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a

---

<sup>4</sup> Many service providers offer different levels of service. Free services provide fewer security and other protections than do paid services. As of the date of this Opinion, the "pro" versions of software and web services generally provide greater protections.

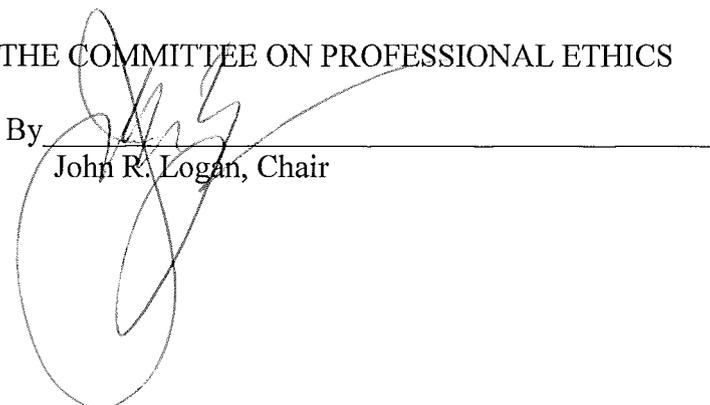
time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Cloud computing online outsourcing is subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are hired by and associated with the lawyer. Therefore, a lawyer must ensure that tasks are delegated to competent and reliable people and organizations. This means that the lawyer outsourcing cloud computing tasks (of transmitting, storing and processing data) must exercise reasonable efforts to select a cloud service provider whose conduct is compatible with the professional obligations of the lawyer and is able to limit authorized access to the data, ensure that the data is preserved (“backed up”), reasonably available to the lawyer, and reasonably safe from unauthorized intrusion.

In summary, the use of cloud computing is a growing trend in many industries and professions, including law. Lawyers may use cloud services in their practice to promote mobility, flexibility, organization and efficiency. However, lawyers must be conscientious to comply with the duties imposed by the Rules to knowledgeably and competently maintain confidentiality and supervisory standards. The Rules require that lawyers make reasonable efforts to meet their obligations to preserve the confidentiality of client information and to confirm that any third-party service provider is likewise obligated.<sup>5</sup>

THE COMMITTEE ON PROFESSIONAL ETHICS

By

  
John R. Logan, Chair

---

<sup>5</sup> As of the date of this Opinion, other states have uniformly concluded that cloud computing, as generally defined, is ethically permissible as long as reasonable care is used by the lawyer to ensure access to and the security of the information stored. E.g., AL Ethics Op. 2010-2; AZ Bar Ethics Op. 09-04 (2009); CA Ethics Op. 2010-179; FL Bar Ethics Op. 06-1 (2006); IA Ethics O. 11-01 (2011); IL Bar Ethics Op. 10-01 (2009); MA Bar Ethics Op. 12-03 (2012); ME Bar Ethics Op. 194 (2008); NH Bar Ethics Op. 2012-13/4 (2012); NC Bar Ethics Op. 6 (2011); ND Bar Ethics Op. 99-03; NJ Bar Ethics Op. 107 (2006); NV Bar Ethics Op. 33 (2006); NY State Bar Ethics Op. 842 (2010); OR Bar Ethics Op. 2011-188 (2011); PA Bar Ethics Op. 2011-200 (2011); VA Ethics Op. 1818 (2005); VT Ethics Op. 2003-03 (2003).

**ATTACHMENT F:**  
**Florida**

**PROFESSIONAL ETHICS OF THE FLORIDA BAR**  
**Opinion 12-3**  
**(January 25, 2013)**

Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

Note: This opinion was affirmed by the Board of Governors with slight modification on July 26, 2013.

**RPC:** 4-1.6

**Opinions:** 10-2, 07-2, Alabama 2010-02, Arizona 09-04, Iowa 11-01, Nevada 33, New York State 842, Pennsylvania 2011-200

The Professional Ethics Committee has been directed by The Florida Bar Board of Governors to issue an opinion regarding lawyers' use of cloud computing. "Cloud computing" is defined as "Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources."<sup>1</sup> It is also defined as "A model of computer use in which services stored on the internet are provided to users on a temporary basis."<sup>2</sup> Because cloud computing involves the use of a third party as a provider of services and involves the storage and use of data at a remote location that is also used by others outside an individual law firm, the use of cloud computing raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers.

In other words, cloud computing involves use of an outside service provider which provides computing software and data storage from a remote location that the lawyer accesses over the Internet via a web browser, such as Internet Explorer, or via an "app" on smart phones and tablets. The lawyer's files are stored at the service provider's remote server(s). The lawyer can thus access the lawyer's files from any computer or smart device and can share files with others. Software is purchased, maintained, and updated by the service provider. Many lawyers and others are computing "in the cloud" because of convenience and potential cost savings.

The main concern regarding cloud computing relates to confidentiality. Lawyers have an obligation to maintain as confidential all information that relates to a client's representation, regardless of the source. Rule 4-1.6, Rules Regulating The Florida Bar. A lawyer may not voluntarily disclose any information relating to a client's representation without either application of an exception to the confidentiality rule or the client's informed consent. *Id.* A lawyer has the obligation to ensure that confidentiality of information is maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services. *See*, Florida Ethics Opinion 07-2 and 10-2.

Additionally, this Committee has previously opined that lawyers have an obligation to remain current not only in developments in the law, but also developments in technology that affect the practice of law. Florida Ethics Opinion 10-2. Lawyers who use cloud computing therefore have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations.

Other states that have addressed the issue of cloud computing have generally determined that there are ethics concerns regarding confidentiality of information, but that a lawyer may compute via the cloud if the lawyer takes reasonable steps. *See, e.g.*, Alabama Ethics Opinion 2010-02 (Lawyer may outsource storage of client files through cloud computing if

they take reasonable steps to make sure data is protected); Arizona Ethics Opinion 09-04 (2009) (Lawyer may use online file storage and retrieval system that enables clients to access their files over the Internet, as long as the firm takes reasonable precautions to protect confidentiality of the information); Iowa Ethics Opinion 11-01 (2011) (Appropriate due diligence a lawyer should perform before storing files electronically with a third party using SaaS (cloud computing), includes determining that the lawyer will have adequate access to the stored information, the lawyer will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider); Nevada Formal Ethics Opinion 33 (2006) (Attorney may store client files electronically on a remote server controlled by a third party as long as the firm takes precautions to safeguard confidential information such as obtaining the third party's agreement to maintain confidentiality); New York State Bar Ethics Opinion 842 (2010) (Lawyer may use an online computer data storage system to store client files provided the attorney takes reasonable care to maintain confidentiality, and the lawyer must stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); and Pennsylvania Ethics Opinion 2011-200 ("An attorney may ethically allow client confidential material to be stored in 'the cloud' provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks").

This Committee agrees with the opinions issued by the states that have addressed the issue. Cloud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it. As indicated by other states that have addressed the issue, lawyers must perform due diligence in researching the outside service provider(s) to ensure that adequate safeguards exist to protect information stored by the service provider(s). New York State Bar Ethics Opinion 842 suggests the following steps involve the appropriate due diligence:

- Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

Of particular practical assistance is Iowa Ethics Opinion 11-01. As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates "any proprietary or user rights" over the data the lawyer stores with the service provider. It also suggests that the lawyer determine whether the information is

password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. It further suggests that the lawyer consider whether the information stored via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via "the cloud."

This Committee agrees with the advice given by both Iowa and New York State. Additionally, this Committee believes that the lawyer should consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information.

In summary, lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

---

1 *Collins English Dictionary - Complete & Unabridged 10th Edition*. HarperCollins Publishers. 10 Sep. 2012. <Dictionary.com  
<http://dictionary.reference.com/browse/cloud%20computing> > .

2 Id.

[Revised: 07-30-2013]

**ATTACHMENT G:**  
**Iowa**



# THE IOWA STATE BAR ASSOCIATION

## Committee on Ethics and Practice Guidelines

Nick Critelli, J.D. Chair  
Timothy Sweet, J.D.  
Marion James, J.D.  
David Phipps, J.D.  
Maureen Heffernan, J.D.  
J.C. Salvo, J.D.

Mark J. Wiedenfeld, J.D.  
Andrew Heiting-Doane, J.D.  
Troy A. Howell, J.D.  
Robert Waterman J.D. ex officio  
Dwight Dinkla, J.D. ex officio

September 9, 2011

Mr. Dwight Dinkla J.D.  
Executive Director  
Iowa State Bar Association  
625 East Court  
Des Moines, IA 50309

RE: Ethics Opinion 11-01 Use of Software as a Service – Cloud  
Computing

Dear Mr. Dinkla,

The Committee has been asked to address whether a lawyer or law firm may utilize what is known as “software as a service” commonly referred to as “SaaS”. The American Bar Association’s Legal Technology Resource Center explains SaaS as follows:

SaaS is distinguished from traditional software in several ways. Rather than installing the software to your computer or the firm's server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the Internet. Data are stored in the vendor's data center rather than on the firm's computers. Upgrades and updates, both major and minor, are rolled out continuously.... SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up-front.

Because SaaS involves storing client information on computer servers that are not owned and operated by the lawyer or law firm, lawyers have questioned whether SaaS can be used in light of Iowa Rule of Professional Conduct 32:1.6 Comment [17]

---

317 Sixth Avenue  
Des Moines, IA 50309  
Phone: 515-243-3122  
E-Mail: Nick@CritelliLaw.com

Rule 32:1.6 [Comment 17] states:

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

We believe the Rule establishes a reasonable and flexible approach to guide a lawyer's use of ever-changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.

Access to stored data and data protection should be taken into consideration when performing due diligence. Whatever form of SaaS is used, the lawyer must ensure that there is unfettered access to the data when it is needed. Likewise the lawyer must be able to determine the nature and degree of protection that will be afforded the data while residing elsewhere.

It is beyond the Committee's ability to conduct a detailed information technology analysis regarding accessibility and data protection used by the presently available SaaS services. Even if we had that ability our analysis would soon be outdated. Instead we prefer to give basic guidance regarding the implementation of the standard described in Comment 17.

### **Accessibility**

We suggest that lawyers intending to use SaaS, or other information technology services that store the lawyer's work product and client information on servers that are not owned by the lawyer, should ask the following questions:

*1. Access:*

Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?

*2. Legal Issues:*

Have I performed “due diligence” regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended by others in the field? What country and state are they located and do business in? Does their end user’s licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?

*3. Financial Obligation:*

What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become the property of the SaaS company or is the data destroyed?

*4. Termination:*

How do I terminate the relationship with the SaaS company? What type of notice does the EULA require. How do I retrieve my data and does the SaaS company retain copies?

### **Data Protection**

In addition to the concepts covered above, lawyers intending to use SaaS should also perform due diligence regarding the degree of protection that will be afforded the data:

*1. Password Protection and Public Access:*

Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?

*2. Data Encryption:*

Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?

### **Lawyer’s Use of Information Technology Due Diligence Services**

The Committee recognizes that performing due diligence regarding information technology can be complex and requires specialized knowledge and skill. This due diligence must be performed by individuals who possess both the requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct. The Committee believes that a lawyer may discharge the duties created by Comment 17 by relying on the due diligence services of independent companies, bar associations or

other similar organizations or through its own qualified employees.

For the Committee,



NICK CRITELLI, Chair  
Iowa State Bar Association  
Ethics and Practice Guidelines Committee

**ATTACHMENT H:**  
**Maine**

# Opinion #207. The Ethics of Cloud Computing and Storage

## Issued by the Professional Ethics Commission

Date Issued: January 8, 2013

### Question

Is it ethical for Maine attorneys to use cloud computing and storage for client matters?

### Answer

Yes, assuming safeguards are in place to ensure that the attorney's use of this technology does not result in the violation of any of the attorney's obligations under the various Maine Rules of Professional Conduct. While the technology is perpetually renewing and reinventing itself, cloud computing triggers the same ethical obligations that lawyers always have owed to their clients. With the expansion of remote data storage and processing services comes the need to observe the same, previously established ethical obligations attorneys always have followed in caring for client information.

So-called "cloud computing" includes any software and/or hardware package that allows a lawyer to transmit, manipulate, store, and retrieve data off the lawyer's premises – in the proverbial clouds – rather than on the hard drive seated at the lawyer's office. It includes platforms like web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs, to name but a few examples.

The American Bar Association ("ABA") canvassed the decisions of state ethics bodies across the nation and listed Maine as one of 13 states to have considered and formally approved attorney use of cloud computing and storage.

<http://www.americanbar.org/groups/departments/offices/legaltechnologyresources/resources/chart/sfyis/cloud-ethics-chart.html> December 21, 2012. The ABA cited Opinion #194 and noted that the Maine Professional Ethics Commission did not squarely address the cloud in that Opinion, but addressed issues similar enough to cover the ethical implications of using cloud computing and storage too. In a recent "Enduring Ethics Opinion" email, the Commission noted that Opinion #194 remained a proper opinion under the Maine Rules of Professional Conduct, even though it was rendered under the former Bar Rules. The Commission further observed that the conclusion reached in Opinion #194 translates to cloud computing and storage, just as the ABA had suggested. However, at the request of Maine attorneys, the Commission has now elected to remove any uncertainty at this point by squarely and formally addressing the issue.

There is another Opinion of the Maine Professional Ethics Commission that should be considered as a precursor to Opinion #194 and this Opinion. Prompted by the increasing shift

from paper hardcopies to electronic data, the Commission issued Opinion #183 on January 28, 2004. The Opinion answered the question whether an attorney is obligated to keep a paper copy of correspondence if that correspondence is converted to an electronic format and stored on a computer. Analyzing then applicable Maine Bar Rules 3.5(a) and 3.6(a) & (e) and Opinions #74 & #120, the Commission concluded that the ethics rules did not require the attorney to retain a paper copy in addition to the electronic one, but only if certain conditions are met. Those conditions generally ensure that the electronic format does not make the correspondence any less accessible to the client than a paper document. Note, however, that M. R. Prof. Conduct 1.15(f) states that there is an obligation now to retain and safeguard client records that have “intrinsic value in the particular version, such as original signed documents,” rather than destroy them after conversion to an electronic format.

Four years later, in 2008, the Commission addressed in Opinion #194 the ethics of transmitting electronic recordings – presumably the lawyer’s dictated correspondence, briefs and the like about the client’s confidential information – for off-site transcription and transferring client files in the form of the electronic data off-site for backup storage. The Commission relied on then applicable Maine Bar Rules 3.6(a) & (h) and 3.13(c), as well as Opinions #74 & #134, to conclude that “with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the attorney’s direct control or supervision without violating the attorney’s ethical obligation to maintain client confidentiality.” The 2008 version of Maine Bar Rule 3.6(a) & (h) can be found in current Maine Professional Conduct Rules 1.1 and 1.6, and former Maine Bar Rule 3.13(c) translates to current Maine Professional Conduct Rule 5.3.

What changes with evolving technology like cloud computing is not the overriding ethical constraints on counsel, but how those constraints are satisfied with respect to new challenges presented by that technology. Commentators on the ethics implications of cloud computing and the Maine Rules of Professional Conduct themselves reveal several rules implicated by the use of this technology:

- Rule 1.1 (competence)
- Rule 1.3 (diligence)
- Rule 1.4 (communications with client)
- Rule 1.6 (confidentiality)
- Rule 1.15 (safeguarding client property)
- Rule 1.16 (terminating representation)
- Rule 1.17 (sale of practice)
- Rule 5.3 (supervision of third parties)

Ethics commissions in other jurisdictions and legal scholars have written extensively on the nuts and bolts of acting ethically with cloud computing, including providing checklists for practitioners. *See, e.g.*, Pennsylvania Formal Opinion 2011-200; North Carolina 2011 Formal Opinion #6 (January 27, 2012); The American Bar Association, “Ethical Challenges on the Horizon: Confidentiality, Competence, and Cloud Computing,” 2012. For the purposes of this Opinion, some of the more salient safeguards Maine counsel should adopt in an effort to satisfy the Maine Rules of Professional Conduct in connection with cloud usage include several internal policies and procedures:

1. backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
2. installing a firewall to limit access to the firm’s network;
3. limiting information that is provided to others to what is required, needed, or requested;
4. avoiding inadvertent disclosure of information;
5. verifying the identity of individuals to whom the attorney provides confidential information;
6. refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
7. protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
8. implementing electronic audit trail procedures to monitor who is accessing the data;
9. creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data; and
10. educating and training employees of the firm who use cloud computing to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

*See* Pennsylvania Formal Opinion 2011-200.

In dealing with third-party vendors of cloud computing services or hardware, additional safeguards Maine counsel should adopt include the following considerations made relevant by the Maine Rules of Professional Conduct.

1. Inclusion in the [cloud computing] . . . vendor’s Terms of Service or Service Level Agreement, or in a separate agreement between the [cloud computing] . . . vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer’s professional responsibilities.
2. If the lawyer terminates use of the [cloud computing] . . . product, the [cloud computing] . . . vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor’s software or source code.

3. The [cloud computing] . . . vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
4. Careful review of the terms of the law firm's user or license agreement with the [cloud computing] . . . vendor including the security policy.
5. Evaluation of the [cloud computing] . . . vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.
6. Evaluation of the extent to which the [cloud computing] . . . vendor backs up hosted data.

North Carolina 2011 Formal Opinion #6 (January 27, 2012)(internal citations omitted).

More specifically, the attorney should ensure that the vendor of cloud computing services or hardware

1. explicitly agrees that it has no ownership or security interest in the data;
2. has an enforceable obligation to preserve security;
3. will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
4. has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
5. provides the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed;
6. will host the firm's data only within a specified geographic area. If the data is 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 Maine;
7. provides the ability for the law firm, on demand, to get data from the vendor's or third-party data hosting company's servers for the firm's own use or for in-house backup.

*See* Pennsylvania Formal Opinion 2011-200.

These lists are not intended to be exhaustive or to convey a "safe harbor" for counsel in all instances of cloud computing. The proprietary cloud options available and the dynamic nature of the technology make it impossible to list criteria that apply to all situations for all time. The North Carolina Ethics Committee aptly articulated the measure of an attorney's appropriately discharging all professional ethical duties owed to the client while using cloud technologies:

[W]hile the duty of confidentiality applies to lawyers who choose to use technology to communicate, "this obligation does not require that a lawyer use only infallibly secure methods of communication." RPC 215. Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client

information and the lawyer must advise effected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality.

\* \* \*

In light of the above, the Ethics Committee concludes that a law firm may use [cloud computing] . . . if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of [cloud computing] . . . that the lawyer is required to apply when representing clients.

North Carolina 2011 Formal Opinion #6 (January 27, 2012).

Furthermore, the reasonable care standard for ethical conduct requires attorneys' periodic education on computer technology as it changes and as it is challenged by and reacts to additional indirect factors such as third party hackers or technical failures.

**ATTACHMENT I:**  
**Massachusetts**

# Ethics Opinions

## Opinion 12-03

**Summary:** A lawyer generally may store and synchronize electronic work files containing confidential client information across different platforms and devices using an Internet based storage solution, such as "Google docs," *so long as* the lawyer undertakes reasonable efforts to ensure that the provider's terms of use and data privacy policies, practices and procedures are compatible with the lawyer's professional obligations, including the obligation to protect confidential client information reflected in Rule 1.6(a). A lawyer remains bound, however, to follow an express instruction from his or her client that the client's confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client's express consent to do so.

**Facts:** A lawyer ("Lawyer") wishes to store and synchronize the electronic work files that he creates in the course of his law practice across multiple computers and devices (*e.g.*, smartphones, iPads, *etc.*) so that he can access them remotely. Some of the work files contain privileged or other confidential client information. Lawyer is considering several potential solutions to address his needs, including storing and synchronizing his electronic files remotely using a third-party service that is accessible through the Internet, such as "Google docs." As described by Google, Google docs is a private service that permits users to store their documents and other data on Google's servers and access that information remotely over the Internet using multiple devices and platforms. Numerous other "cloud" based storage options, such as Microsoft's "Windows Azure," Apple's "iCloud," and Amazon.com's "S3" service, exist. The issue presented is whether it would violate Lawyer's obligations under the Massachusetts Rules of Professional Conduct to store confidential client information using Google docs or some other Internet based storage solution, and to synchronize his computers and other devices that contain or access such information over the Internet.

**Discussion:** Rule 1.6 of the Massachusetts Rules of Professional Conduct governs the confidentiality of client information. Subsection (a) of Rule 1.6 provides, in relevant part, that "[a] lawyer shall not reveal confidential information relating to the representation of a client unless the client consents after consultation...." The duty of confidentiality dictated by Rule 1.6 (as well as other rules) imposes upon Lawyer the obligation to avoid using means of communication with the client that pose an unreasonable risk of inadvertent disclosure to third persons.

In this context, the question posed is whether Lawyer's use of Google docs or another Internet based data storage service provider, which carries with it a small, but genuine risk of unauthorized access or interception, presents an unreasonable risk of inadvertent disclosure and, therefore, violates Rule 1.6(a).

The Committee on Professional Ethics previously has addressed issues of client confidentiality posed by a lawyer's use of the Internet and remote access capabilities. For example, in Opinion

00-01, the Committee concluded that a lawyer's use of unencrypted Internet e-mail to engage in confidential communications with his or her client does not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances. We said, in relevant part,

[i]t is the Committee's opinion that the use of unencrypted Internet e-mail for the purpose of transmitting confidential or privileged client communications does not, in most instances, constitute a violation of any applicable ethical rule, including Rule 1.6. The Committee reaches this conclusion primarily because it believes that both the lawyer and the client typically have a reasonable expectation that such communications will remain legally and effectively private. *See, e.g.*, 18 U.S.C.A. 2510, *et seq.* (the "Electronic Communications Privacy Act"). The technological possibility that a privileged or confidential e-mail communication could be intercepted in disregard of federal law does not diminish that expectation. Other standard forms of communication, including the telephone and the United States mail, also carry with them some risk of interception. Legal prohibitions on the interception of private telephone calls and letters, however, generally provide protection against unauthorized disclosure sufficient to make those means of communication reasonably secure for purposes of Rule 1.6(a). The Committee believes that, in light of statutes such as the Electronic Communications Privacy Act, the same reasoning now applies to unencrypted Internet e-mail.

Similarly, in Opinion 05-04, the Committee concluded that a law firm may provide a third-party software vendor with remote access to confidential client information stored on the firm's computers for the purpose of allowing the vendor to support and maintain a computer software application utilized by the law firm *so long as* the law firm undertakes "reasonable efforts" to ensure that the conduct of the software vendor "is compatible with the professional obligations of the lawyer[s]," including the obligation to protect confidential client information reflected in Rule 1.6(a). The Committee stated that "reasonable efforts" in the circumstances would include, among other things,

(a) notifying the vendor of the confidential nature of the information stored on the firm's servers and in its document database; (b) examining the vendor's existing policies and procedures with respect to the handling of confidential information; (c) obtaining written assurance from the vendor that confidential client information on the firm's computer system will only [be] utilized solely for technical support purposes and will be accessed only on an "as needed" basis; (d) obtaining written assurance from the vendor that the confidentiality of all client information will be respected and preserved by the vendor and its employees; and (e) drafting and agreeing upon additional procedures for protecting any particularly sensitive client information that may reside on the firm's computer system, to the extent necessary.

The Committee believes that the reasoning set forth in Opinion 00-01 and Opinion 05-04 generally would allow Lawyer also to use Google docs or some other Internet based data storage service provider to store confidential client information, and to synchronize data using that provider over the Internet. More specifically, the Committee believes that the use of an Internet based service provider to store confidential client information would not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances *so long as* Lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations, including the obligation to protect

confidential client information reflected in Rule 1.6(a). "Reasonable efforts" by Lawyer with respect to such a provider would include, in the Committee's opinion:

(a) examining the provider's terms of use and written policies and procedures with respect to data privacy and the handling of confidential information;

(b) ensuring that the provider's terms of use and written policies and procedures prohibit unauthorized access to data stored on the provider's system, including access by the provider itself for any purpose other than conveying or displaying the data to authorized users;

(c) ensuring that the provider's terms of use and written policies and procedures, as well as its functional capabilities, give the Lawyer reasonable access to, and control over, the data stored on the provider's system in the event that the Lawyer's relationship with the provider is interrupted for any reason (*e.g.*, if the storage provider ceases operations or shuts off the Lawyer's account, either temporarily or permanently);

(d) examining the provider's existing practices (including data encryption, password protection, and system back ups) and available service history (including reports of known security breaches or "holes") to reasonably ensure that data stored on the provider's system actually will remain confidential, and will not be intentionally or inadvertently disclosed or lost; and

(e) periodically revisiting and reexamining the provider's policies, practices and procedures to ensure that they remain compatible with Lawyer's professional obligations to protect confidential client information reflected in Rule 1.6(a).

Consistent with its prior opinions, the Committee further believes that Lawyer remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet, and that he should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so.<sup>[1]</sup>

Applying its conclusions to Google docs, Lawyer's proposed Internet based data storage solution, the Committee observes that Google has adopted written terms of service and a privacy policy for users of Google docs (*see generally* <http://www.google.com/google-d-s/terms.html>) that reference and incorporate various other Google policies. Among other things, Google represents that data stored on Google docs is "private" and "password protected," but can be voluntarily shared by the user with others or published to the World Wide Web. The Committee further observes that Google docs and other Internet based storage solutions, like many, if not most, remotely accessible software systems and computer networks, are not immune from attack by unauthorized persons or other forms of security breaches. *See, e.g.*, "How Safe Are Your Google Docs", found at <http://www.odesk.com/blog/2010/05/how-safe-are-your-google-docs>; and "Can You Trust Your Data To Amazon, Other Storage Cloud Providers?", found at <http://www.networkworld.com/supp/2008/ndc3/051908-cloud-storage.html>.

The foregoing policies, protections and resources are referenced by the Committee solely for informational purposes. Ultimately, the question of whether the use of Google docs, or any other

Internet based data storage service provider, is compatible with Lawyer's ethical obligation to protect his clients' confidential information is one that Lawyer must answer for himself based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment.

*This opinion was approved for publication by the Massachusetts Bar Association's House of Delegates on May 17, 2012.*

<sup>[1]</sup> The American Bar Association and the bar associations of various states also have addressed the ethical implications of using Internet-based software and data storage services, either formally or provisionally. *See, e.g.*, American Bar Assoc. Commission on Ethics 20/20 "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology," dated September 20, 2010; New York State Bar Association Committee on Professional Ethics Opinion 842, dated September 10, 2010; California State Bar Standing Committee on Professional Responsibility and Conduct Proposed Formal Opinion Interim No. 08-0002, approved for public comment in August 2010; Iowa State Bar Association Committee on Ethics and Practice Guidelines Opinion 11-01, dated September 9, 2011; and North Carolina State Bar Ethics Committee Proposed 2011 Formal Ethics Opinion 6, dated October 20, 2011.

**ATTACHMENT J:**  
**Nevada**

STATE BAR OF NEVADA  
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL  
RESPONSIBILITY

**Formal Opinion No. 33**  
**Issued February 9, 2006**

**BACKGROUND**

A Nevada attorney has requested an opinion concerning the application of Supreme Court Rules to the attorney's use of an outside agency to store electronically formatted client information. In the situation posed, the attorney's electronic client files, which contain confidential client information and communications, are stored on a server or other computer device which is physically located and maintained by a third party outside the attorney's direct control and supervision. It is assumed that the attorney can, as part of his or her service contract with the third party, require that all reasonably necessary means be employed by the third party to preserve the confidentiality of the information and to prevent unauthorized access to it and disclosure of it. It is also assumed, however, that employees of the third party agency will, by virtue of their employment, have access, both authorized and unauthorized, to the confidential client information.

**QUESTION PRESENTED**

The committee has revised the question originally presented to more broadly address the lawyer's duty of confidentiality with respect to electronic client information. The question addressed in this opinion is whether a lawyer violates SCR 156 by storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control.

**ANSWER**

The lawyer's duty to protect client confidentiality under Supreme Court Rule 156 is not absolute. In order to comply with the rule, the lawyer must act competently and reasonably to safeguard confidential client information and communications from inadvertent and unauthorized disclosure. This may be accomplished while storing client information electronically with a third party to the same extent and subject to the same standards as with storing confidential paper files in a third party warehouse. If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate SCR 156 simply by contracting with a third party to store the information, even if an unauthorized or inadvertent disclosure should occur.

**SUPREME COURT RULE INTERPRETED**

Supreme Court Rule 156

## AUTHORITIES AND REFERENCES

ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413 (1999).

ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 95-398 (1995).

ABA Committee on Lawyers' Responsibility for Client Protection, *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication* (1986).

ABA Committee on Professional Ethics, Informal Opinion No. 1127 (1970).

Anderson, J.C., *Transmitting Legal Documents over the Internet: How to Protect Your Client and Yourself*, 27 Rutgers Computer & Tech. L.J. 1 (2001).

Annotated Model Rules of Professional Conduct, 5<sup>th</sup> ed. (ABA, 2003), Rule 1.6 and accompanying commentary.

California Standing Committee on Professional Responsibility and Conduct, Formal Opinion number 1971-25.

Hopkins, R.S. & Reynolds, P.R., *Redefining Privacy and Security in the Electronic Communication Age: A Lawyer's Ethical Duty in the Virtual World of the Internet*, 16 Geo. J. Legal Ethics 675 (2003).

Winick, M.L., Burris, B. & Bush, Y.D. *Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications*, 31 Tex. Tech L. Rev. 1225 (2000).

## DISCUSSION

A lawyer must act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information. While a lawyer is not strictly liable for any breach of client confidentiality, his duty includes reasonable precautions to prevent both accidental and unauthorized disclosure. SCR 156; Model Rule 1.6, comment 16. A client, however, may give informed consent to a means of protection that might otherwise be considered insufficient. For purposes of this opinion, however, it is presumed that the client has not waived any right to confidentiality or consented to a means of protection that would otherwise violate the Supreme Court Rules absent informed consent.

Opinions directly addressing this issue, particularly with respect to electronic data, are scarce and somewhat outdated given the recent advances in electronic communications and data processing. Available opinions and commentary added to Model Rule 1.6 by

the ETHICS 2000 amendments, however, clearly support the answer stated in this opinion.

The ABA Committee on Professional Ethics, in Informal Opinion No. 1127 (1970) (interpreting former Canon 37), addressed the question whether confidential client information could be stored in a central computer facility, in which the information would be accessible to, but would not necessarily be accessed by, employees of the facility. The committee determined that so long as arrangements were made so that the information transmitted to the data processor was kept in confidence, and the employees of the law firm and the data processor did not permit disclosure to any unauthorized person, then there was no violation of the lawyer's duty of confidentiality. The required "arrangements", in the committee's opinion, consisted of competence and reasonable care in 1) the selection of the third party contractor and 2) an express contractual requirement that the contractor and its employees keep the information confidential and protected from unauthorized access or disclosure.

In Formal Opinion number 1971-25, the California Standing Committee on Professional Responsibility and Conduct responded differently, but to a somewhat different question. That opinion addressed an attorney's transmission of confidential client information, without prior client consent, to a "data processing center for bookkeeping, billing, accounting, and statistical purposes." *Id.* at p. 2. The question there was somewhat different than that presented here in that it was presumed that at least one of the purposes of the transmission of the information to the "data processing center" would necessitate the disclosure of confidential client information to a person or persons not employed, supervised or controlled by the attorney. The committee concluded that without the client's consent, the disclosure of confidential information to a third person in such circumstances violates the attorney's duty of confidentiality.

The issue presented here is more similar to that involved in the ABA committee opinion. The use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney's employ. The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a "hacker" who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files. The question in either case is whether the attorney acted reasonable and competently to protect the confidential information. The California opinion is thus distinguished by the presumption underlying that opinion that the attorney could exercise no control whatsoever over the confidential information in the hands of the third party contractor.

Subsequent ABA opinions concerning client confidentiality in the electronic age have to some degree reflected the evolution of electronic technology itself. In 1986, an ABA committee issued a report cautioning lawyers against electronic client communications and concluded that an attorney should not communicate with clients electronically without first obtaining the client's informed consent or being reasonably assured of the

security of the electronic system in question. ABA Committee on Lawyers' Responsibility for Client Protection, *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication* (1986). The committee did not ban all such communication, but rather described the lawyer's obligation in this regard as an affirmative duty to competently investigate the electronic communications system and form a reasonable conclusion as to its security. *Id.*

The ABA Committee addressed an issue much closer to that discussed here in Formal Opinion number 95-398, and concluded that a lawyer may give a computer maintenance company access to confidential information in client files, but that in order to comply with the obligation of client confidentiality, he or she "must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information." The ABA Committee recognized in that opinion the growing practicality and availability of third party electronic data services, but clearly concluded that the duty of confidentiality is not breached so long the attorney is reasonable and competent in the creation and management of the outside contractor arrangement.

In a later formal opinion, the ABA Committee continued this trend and retreated substantially from the 1986 opinion concerning the encryption of e-mail. That opinion concluded that sending confidential client communications by unencrypted email does not violate the lawyer's duty of confidentiality because unencrypted email still affords a reasonable expectation of privacy from both legal and technological standpoints. ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413 (1999). The committee left open the likelihood, however, that cases of particularly sensitive client communications may require extraordinary security precautions, since the reasonableness and competence of the lawyer's actions must be judged in the context of the relative sensitivity of the particular confidential information or communication at stake. See Model Rule 1.6, comments 16 and 17.

Nearly all state bar associations and committees addressing the issue have adopted the ABA's 1999 approach to email communications. Hopkins & Reynolds at 677-78; Winich, Burris & Bush at 1252-1254. Commentators have argued that further advances in technology will increase the lawyer's obligation with respect to electronic client communications and information and that "reasonable" action to protect client confidentiality already may include encryption, virus protection and other similar security measures as they become more efficient and cost effective, and as electronic communications and data storage may eventually be found to afford less than a reasonable expectation of privacy. Hopkins & Reynolds at 691.

The ABA, at least for now, has continued the course set in the 1999 formal opinion, adding two new comments to Model Rule 1.6 to reinforce the view that electronic communications and information require no special security or confidentiality measures that would not otherwise be required in communication in a more traditional format. The new comments are:

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

The previous ABA opinions and the new comments to Rule 1.6 clearly evidence the ABA's policy to treat electronic client communications and information according to existing rules and not to hold an attorney responsible for a breach of client confidentiality, or for storing client information in such a manner that the breach is possible, so long as the attorney:

1. Exercises reasonable care in the selection of the third party contractor, such that the contractor can be reasonably relied upon to keep the information confidential; and
2. Has a reasonable expectation that the information will be kept confidential; and
3. Instructs and requires the third party contractor to keep the information confidential and inaccessible.

## CONCLUSION

The ETHICS 2000 comments to Model Rule 1.6, and decisions under the Supreme Court Rules, generally apply traditional rules of confidentiality to new forms of communication and document storage. Thus, the practice at issue here can be compared to the storage of paper documents containing confidential client information in a warehouse operated by company or person outside the lawyer's direct control. In such a case, the same risk exists that an employee of the warehouse, or some other person, will access and perhaps disclose the information without authorization. But neither the Model Rules nor the Supreme Court Rules would prohibit the third party storage arrangement altogether. Rather, they require the attorney to act reasonably and competently to protect the information from inadvertent and unauthorized access and disclosure.

It is therefore the opinion of this committee that an attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third party declines to agree to keep the information confidential, then the attorney violates SCR 156 by transmitting the data to the third party. But if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent.

The client may consent to the storage of confidential information in any manner. It is clear that SCR 156 and the Supreme Court Rules generally would prefer that the lawyer obtain the client's informed consent before transmitting confidential information to third parties in any case, but the rules do not prohibit the storage of electronic client information, without client consent, in any manner that complies with the lawyer's duty to competently and reasonably safeguard the confidentiality of client information.

**NOTE: This opinion is issued by the Standing Committee on Ethics and Professional Responsibility of the State Bar of Nevada pursuant to SCR 225. It is advisory only. It is not binding on the courts, the State Bar of Nevada, its Board of Governors, any person or tribunal charged with regulatory responsibility, or any other member of the State Bar of Nevada.**

**ATTACHMENT K:**  
**New Hampshire**

# **Ethics Committee Advisory Opinion #2012-13/4**

## **The Use of Cloud Computing in the Practice of Law**

**By the NHBA Ethics Committee**

*This opinion was submitted for publication by the NHBA Board of Governors at its February 21, 2013 meeting.*

### **RULE REFERENCES:**

Rule 1.0(e)  
Rule 1.1  
Rule 1.6  
Rule 1.15  
Rule 2.1  
Rule 5.3

### **SUBJECTS:**

Informed Consent  
Competence  
Confidentiality of Information  
Safekeeping Property  
Responsibilities Regarding Nonlawyer Assistants

### **ANNOTATION**

The internet has changed the practice of law in many ways, including how data is stored and accessed. "Cloud computing" can be an economical and efficient way to store and use data. However, a lawyer who uses cloud computing must be aware of its effect on the lawyer's professional responsibilities. The NHBA Ethics Committee adopts the consensus among states that a lawyer may use cloud computing consistent with his or her ethical obligations, as long as the lawyer takes reasonable steps to ensure that sensitive client information remains confidential.

### **INTRODUCTION**

As technology becomes more pervasive in the practice of law, lawyers encounter cloud computing. Cloud computing is the storage of data and the ability to run applications on remote servers over the Internet, rather than on a desktop computer or a server in a law office. Cloud computing is already a part of many devices and services which lawyers use, including smart phones, stored emails, and online data storage services such as Google Docs, Microsoft Office 365, and DropBox.<sup>1</sup>

Cloud computing offers many benefits. Typically, it is purchased on a subscription basis, usually for a monthly fee, which reduces upfront licensing costs.<sup>2</sup> The provider takes over the responsibility for keeping up with new technology and software updates, while the lawyer enjoys access to all the data stored in the cloud from any location which has Internet access. Increased mobility and accessibility, however, may come with the loss of immediate control over the stored or transmitted data. Like any middleman, the provider of cloud computing adds a layer of risk between the lawyer and sensitive client information.

A lawyer who uses cloud computing should therefore be aware of its effect on the lawyer's professional responsibilities. The consensus among states is that a lawyer may use cloud computing consistent with his or her ethical obligations. To date, every state bar association that has issued an opinion on using cloud computing has said that it is permissible, as long as the lawyer takes reasonable steps to ensure that sensitive client information remains confidential.<sup>3</sup> Several rules are implicated by the use of cloud computing. This opinion discusses cloud computing, but not emails. The two are separate and raise different issues. As explained in the Pennsylvania Bar Association's opinion on cloud computing, email presents unique risks and challenges which must be addressed and mitigated separately: these include "confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware."<sup>4</sup>

#### **Rule 1.1. Competence**

A lawyer must provide competent legal representation, and minimal competence requires a lawyer to perform the techniques of practice with skill. Rule 1.1 (b) (2). Techniques of practice include the way a client's information and the lawyer's work product are maintained, stored, and organized.<sup>5</sup> As the revised Comment [6] to the ABA Model Rule 1.1 states, a lawyer must "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology."<sup>6</sup> The comment was revised recently in response to "the sometimes bewildering pace of

technological change," including cloud computing.<sup>7</sup> A competent lawyer using cloud computing must understand and guard against the risks inherent in it.

There is no hard and fast rule as to what a lawyer must do with respect to each client when using cloud computing. The facts and circumstances of each case, including the type and sensitivity of client information, will dictate what reasonable protective measures a lawyer must take when using cloud computing. The same rationale applies to the transmission of metadata, as discussed in NH Bar Ethics Op. 2008-2009/4 on the disclosure, review, and use of metadata in electronic materials.

Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes.<sup>8</sup>

#### **Rule 1.6. Confidentiality of Information and Rule 1.0 (e). Informed Consent**

Protecting client confidences is one of the most significant obligations imposed upon lawyers and is the core of the attorney-client relationship. Rule 1.6(a) states that "[a] lawyer shall not reveal information relating to the representation of a client[.]" Confidentiality applies not only to matters communicated in confidence by the client, but also to all information related to the representation, whatever its source. See 2004 ABA Model Rule Comment [3]. A lawyer may reveal such information if the client gives informed consent or if the disclosure is impliedly authorized.<sup>9</sup>

As cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider of cloud computing services has adequate safeguards. Recent revisions to Comment [16] to the ABA Model Rule 1.6 note that "if the lawyer has made reasonable efforts to prevent the access or disclosure" of confidential information, then the unauthorized access to, or the inadvertent or unauthorized disclosure of, client information does not constitute a violation of a lawyer's duty of confidentiality.<sup>10</sup>

The comment sets forth a number of "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" to prevent such unauthorized access or disclosure. These factors "include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."<sup>11</sup>

Not all information is alike. For example, where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent. "'Informed consent' denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." Rule 1.0 (e). The material risks and reasonably available alternatives will of course vary by client, scope of representation, the sensitivity of the stored or transmitted information, provider, and other considerations.<sup>12</sup> But if the information is highly sensitive, consent of the client to use cloud computing may be necessary.

#### **Rule 1.15. Safekeeping Property**

"Property of clients or third persons which a lawyer is holding in the lawyer's possession," other than funds, "shall be identified as property of the client, promptly upon receipt, and safeguarded." Rule 1.15(a). The New Hampshire Supreme Court has held that the contents of a client's file belong to the client and that, upon request, an attorney must provide the client with the file. *Averill v. Cox*, 145 N.H. 328, 339 (2000). Electronic communications are also part of the client's file. NH Bar Ethics Op. 2005-06/3.

Additionally, Rule 1.16(d) of the New Hampshire Rules of Professional Conduct states that, as a condition to termination of representation, a lawyer shall "surrender[] papers and property to which the client is entitled" and only "retain papers relating to the client to the extent permitted by law." In the context of cloud computing, the lawyer must take steps to safeguard data stored in and transmitted through the cloud. What safeguards are appropriate depends on the nature and sensitivity of the data. More particularly, a lawyer must take reasonable steps to ensure that electronic data stored in the cloud is secure and available while representing a client. The data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer to preserve the file: in either case, the lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.

#### **Rule 5.3. Responsibilities Regarding Nonlawyer Assistants**

Cloud computing is a form of outsourcing the storage and transmission of data. What was once a matter of documents and file cabinets is now online.<sup>13</sup> This means that a provider of cloud computing services is, in effect, a nonlawyer retained by a lawyer. As a result, the lawyer must make reasonable efforts to ensure that the provider

understands and is capable of complying with its obligation to act in a manner compatible with the lawyer's own professional responsibilities. N.H. Rule 5.3 (a).

The same rationale applies when, instead of directly engaging a cloud computing provider, a lawyer hires an intermediary, such as an information technology professional or other support staff, to find and engage a provider. As noted in NH Bar Ethics Op. 2011-12/5, "Lawyers regularly engage companies to provide support services. Banks hold client funds; telephone companies carry privileged communications; credit card companies facilitate the payment of bills; computer consultants maintain necessary technology." When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a). Additionally, under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud.

Thus, a lawyer who uses cloud computing must take reasonable steps to ensure that sensitive client information remains confidential and secure.<sup>14</sup> What these steps are depends on the sensitivity of the transmitted information.<sup>15</sup> It bears repeating that a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology. When it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard. As one ethics committee observed, "Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax."<sup>16</sup>

Which providers of cloud computing may be used and what security measures the provider must take are beyond the scope of this opinion. This opinion addresses instead what an attorney may consider when storing data on or transmitting data through the cloud. For recommendations on which cloud computing services to use, see American Bar Association, "Delivering Value and Efficiency with Technology: Effectively Collecting and Managing Data in a Virtual World," p. 12.<sup>17</sup> For more information on which factors to consider when choosing a provider of cloud computing services, see American Bar Association, "Your ABA: Evaluating Cloud-Computing Providers."<sup>18</sup>

#### **Cloud Computing Considerations:**

The issues which an attorney must consider before using a cloud computing service include the following:

1. Is the provider of cloud computing services a reputable organization?
2. Does the provider offer robust security measures? Such measures<sup>19</sup> must include at a minimum password protections or other verification procedures limiting access to the data; safeguards such as data back-up and restoration, a firewall, or encryption; periodic audits by third parties of the provider's security; and notification procedures in case of a breach.<sup>20</sup>
3. Is the data stored in a format that renders it retrievable as well as secure? Is it stored in a proprietary format<sup>21</sup> and is it promptly and reasonably retrievable by the lawyer in a format acceptable to the client? See also PA Bar Ethics Op. 2011-200, p. 9. It bears repeating that, if a client requests a copy of her file, the lawyer has an obligation to provide all files pertinent to representation of that client. NH Bar Ethics Op. 2005-06/3; *Averill*, 145 N.H. at 339-40.
4. Does the provider commingle data belonging to different clients and/or different practitioners such that retrieval may result in inadvertent disclosure?<sup>22</sup>
5. Do the terms of service state that the provider merely holds a license to the stored data, as for example Google's do?<sup>23</sup> Some providers routinely inform those accessing their service that it is the provider—not the user—that "owns" the data.<sup>24</sup> If the provider owns the stored data, the lawyer may run afoul of Rule 1.15, which requires that the client's property "be identified as property of the client." To comply with Rule 1.15, the provider may not "own" the data stored in the cloud.
6. Does the provider have an enforceable obligation to keep the data confidential?
7. Where are the provider's servers located and what are the privacy laws in effect at that location regarding unauthorized access, retrieval, and destruction of compromised data?<sup>25</sup> If the servers are located in a foreign country, do the privacy laws of that country reasonably mirror those of the United States? If the servers are relocated, will the provider notify the lawyer in advance?

8. Will the provider retain the data – and, if so, for how long – when the representation ends or the agreement between the lawyer and provider is terminated for another reason? The data must not be destroyed immediately and without notice or compromised in case of nonpayment.<sup>26</sup>
9. Do the terms of service obligate the provider to warn the lawyer if information is being subpoenaed by a third party, where the law permits such notice? Such a provision may be especially timely given that the Senate Judiciary Committee recently considered, but rejected legislation which would have expanded law enforcement agencies' access to privately stored data.<sup>27</sup>
10. What is the provider's disaster recovery plan with respect stored data? Is a copy of the digital data stored on-site?<sup>28</sup>

The New Hampshire Ethics Committee concurs with the consensus among states that a lawyer may use cloud computing in a manner consistent with his or her ethical duties by taking reasonable steps to protect client data. Granted, a lawyer may not find a provider of cloud computing services whose terms of service address all of the issues addressed above, but it bears repeating, that while a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data is stored and what the service agreement says.<sup>29</sup> Although the New Hampshire Rules of Professional Conduct do not impose a strict liability standard, the duties of confidentiality and competence are ongoing and not delegable. The requirement of competence means that even when storing data in the cloud, a lawyer must take reasonable steps to protect client information and cannot allow the storage and retrieval of data to become nebulous.

---

#### ENDNOTES:

<sup>1</sup> American Bar Association, [Cloud Computing/Software as a Service for Lawyers](#) (last accessed on October 23, 2012). See also PA Bar Ethics Op. 2011-200 and Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1199-1200 (2010).

<sup>2</sup> PA Bar Ethics Op. 2011-200, p. 1.

<sup>3</sup> AL Bar Ethics Op. 2010-02; AZ Bar Ethics Op. 09-04 (2009); CA Bar Ethics Op. 2010-179, p. 3; FL Bar Ethics Op. 06-1 (2006); IA Bar Ethics Op. 11-01 (2011), p. 2; IL Bar Ethics Op. 10-01 (2009), p. 3; ME Bar Ethics Op. 194 (2008); MA Bar Ethics Op. 05-04 (2005); NV Bar Ethics Op. 33 (2006); NJ Bar Ethics Op. 107 (2006); NY Bar Ethics Op. 842 (2010); NC Bar Ethics Op. 6 (2011); ND Bar Ethics Op. 99-03 (1999), p. 3; OR Bar Ethics Op. 2011-188; PA Bar Ethics Op. 2011-200, p. 1; VT Bar Ethics Op. 2003-03; VA Bar Ethics Op. 1818 (2005).

<sup>4</sup> PA Bar Ethics Op. 2011-200, p. 12.

<sup>5</sup> PA Bar Ethics Op. 2011-200, p. 4.

<sup>6</sup> In 2012, the ABA revised Comment [6] to Rule 1.1. American Bar Association Commission on Ethics 20/20, Report to the House of Delegates, Resolution, 105A Revised, p. 3 [www.americanbar.org](http://www.americanbar.org) (last accessed December 27, 2012). On behalf of the New Hampshire Supreme Court's Rules Committee, the Bar's Ethics Committee is currently reviewing the revision to Comment [6]. The proposed revision has not yet been recommended to the Rules Committee or adopted by the Supreme Court. [New Hampshire Rules of Professional Conduct](#) (last accessed December 27, 2012).

<sup>7</sup> American Bar Association Commission on Ethics 20/20, Introduction and Overview, p. 8.

<sup>8</sup> For example, recent Senate amendments to H.R. 2471 (2012) would have amended the Electronic Communications Privacy Act to permit warrantless searches of emails by a number of federal agencies. The amendments were introduced and then withdrawn in the face of widespread criticism, but such legislative uncertainties highlight the need to be aware of changes in technology regulation.

<sup>9</sup> See NH Bar Ethics Op. 2008-2009/4.

<sup>10</sup> American Bar Association Commission on Ethics 20/20, Report to the House of Delegates, Resolution, 105A Revised, p. 5. On behalf of the New Hampshire Supreme Court's Rules Committee, the Bar's Ethics Committee is currently reviewing the revision to Comment [16]. The proposed revision has not yet been recommended to the Rules Committee or adopted by the Supreme Court. [New Hampshire Rules of Professional Conduct](#) (last accessed December 27, 2012).

<sup>11</sup> Id.

<sup>12</sup> PA Bar Ethics Op. 2011-200, p. 7; IA Bar Ethics Op. 11-01 (2001), p. 2.

<sup>13</sup> PA Bar Ethics Op. 2011-200, p. 7.

<sup>14</sup> NH Bar Ethics Op. 2008-2009/4.

<sup>15</sup> IA Bar Ethics Op. 11-01 (2001), p. 2.

<sup>16</sup> N.J. Advisory Committee on Professional Ethics Op. No. 701 (electronic filing systems).

<sup>17</sup> [www.americanbar.org](http://www.americanbar.org) (members of the New Hampshire Bar may contact the Ethics Committee regarding access to the article); see also American Bar Association, [eLawyering in an Age of Accelerating Technology](#) (last accessed January 29, 2013).

<sup>18</sup> <http://www.americanbar.org/newsletter/publications/youraba/201206article12.html> (last accessed on December 3, 2012).

<sup>19</sup> PA Bar Ethics Op. 2011-200, pp. 8-9.

<sup>20</sup> NH law, RSA 359-C:20 (2009), already requires any person doing business in New Hampshire to notify (or cooperate in notifying) those individuals who are affected by any security breach of unencrypted computerized data that contains personal information. See, generally, Gallagher, Callahan & Gartrell, [New Hampshire Mandates Data Breach Notification](#), August 2006, (last accessed on October 23, 2012).

<sup>21</sup> Proprietary formats can only be opened by certain programs or applications. For example, Microsoft Word, which used to save word processing documents in the proprietary .DOC format now saves documents in the .DOCX format, which is supported by multiple applications. See also PA Bar Ethics Op. 2011-200, p. 9.

<sup>22</sup> American Bar Association, "Cloud Computin': A Storm is A-brewin'," p. 26 (members of the New Hampshire Bar may contact the Ethics Committee regarding access to the article).

<sup>23</sup> [Google Terms of Service](#) (last modified March 1, 2012) (last accessed on December 4, 2012); see also MA Bar Ethics Op. 2012-03.

<sup>24</sup> IA Bar Ethics Op. 11-01 (2001), p. 3.

<sup>25</sup> PA Bar Ethics Op. 2011-200, p. 6.

<sup>26</sup> IA Bar Ethics Op. 11-01 (2001), p. 3.

<sup>27</sup> CNet, "[Leahy scuttles his warrantless e-mail surveillance bill](#)," November 20, 2012, (last accessed December 27, 2012); see also CNet, "[Senate bill rewrite lets feds read your e-mail without warrants](#)," November 20, 2012, (last accessed December 27, 2012).

<sup>28</sup> PA Bar Ethics Op. 2011-200, p. 10.

<sup>29</sup> PA Bar Ethics Op. 2011-200, p. 13.

**ATTACHMENT L:**  
**New Jersey**

Advisory Committee on Professional Ethics  
Appointed by the Supreme Court of New Jersey

**Opinion 701**  
**Advisory Committee on Professional Ethics**  
**Electronic Storage And Access of Client Files**

The inquirer asks whether the Rules of Professional Conduct permit him to make use of an electronic filing system whereby all documents received in his office are scanned into a digitized format such as Portable Data Format (“PDF”). These documents can then be sent by email, and as the inquirer notes, “can be retrieved by me at any time from any location in the world.” The inquirer notes that certain documents that by their nature require retention of original hardcopy, such as wills, and deeds, would be physically maintained in a separate file.

In Opinion 692, we set forth our interpretation of the term “property of the client” for purposes of *RPC* 1.15, which then triggers the obligation of a lawyer to safeguard that property for the client. “Original wills, trusts, deeds, executed contracts, corporate bylaws and minutes are but a few examples of documents which constitute client property.” 163 *N.J.L.J.* 220, 221 (January 15, 2001) and 10 *N.J.L.* 154 (January 22, 2001). Such documents cannot be preserved within the meaning of *RPC* 1.15 merely by digitizing them in electronic form, and we do not understand the inquirer to suggest otherwise, since he acknowledges his obligation to maintain the originals of such documents in a separate file.

On the other hand, we also noted in Opinion 692 that a client file will likely contain other documents, such as correspondence, pleadings, memoranda, and briefs, that are not “property of the

client” within the meaning of *RPC* 1.15, but that a lawyer is nevertheless required to maintain at least for some period of time in order to discharge the duties contained in *RPC* 1.1 (Competence) and *RPC* 1.4 (Communication), among others. While traditionally a client file has been maintained through paper records, there is nothing in the *RPCs* that mandates a particular medium of archiving such documents. The paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer’s ability to discharge those duties may very well be enhanced by having client documents available in an electronic form that can be transmitted to him instantaneously through the Internet. We also note the recent phenomenon of making client documents available to the client through a secure website. This also has the potential of enhancing communications between lawyer and client, and promotes the values embraced in *RPC* 1.4.

With the exception of “property of the client” within the meaning of *RPC* 1.15, therefore, and with the important caveat we express below regarding confidentiality, we believe that nothing in the *RPCs* prevents a lawyer from archiving a client’s file through use of an electronic medium such as PDF files or similar formats. The polestar is the obligation of the lawyer to engage in the representation competently, and to communicate adequately with the client and others. To the extent that new technology now enhances the ability to fulfill those obligations, it is a welcome development.

This inquiry, however, raises another ethical issue that we must address. As the inquirer notes, the benefit of digitizing documents in electronic form is that they “can be retrieved by me at any time from any location in the world.” This raises the possibility, however, that they could also be retrieved by other persons as well, and the problems of unauthorized access to electronic platforms and media (i.e. the problems posed by “hackers”) are matters of common knowledge. The availability of sensitive client documents in an electronic medium that could be accessed or intercepted by unauthorized users therefore raises issues of confidentiality under *RPC* 1.6.

The obligation to preserve client confidences extends beyond merely prohibiting an attorney from himself making disclosure of confidential information without client consent (except under such

circumstances described in *RPC* 1.6). It also requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure. Thus, in Opinion 692, we stated that even when a closed client file is destroyed (as permitted after seven years), “[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties.” 163 *N.J.L.J.* 220, 221 (January 15, 2001) and 10 *N.J.L.* 154 (January 22, 2001). Similarly, in ACPE Opinion 694 and CAA Opinion 28 (joint opinion), we joined with the Committee on Attorney Advertising in finding that two separate firms could not maintain shared facilities where “the pervasive sharing of facilities by the two separate firms as described in the Agreement gives rise to a serious risk of a breach of confidentiality that their respective clients are entitled to.” 174 *N.J.L.J.* 460 and 12 *N.J.L.* 2134 (November 3, 2003).

And in Opinion 515, we permitted two firms to share word processing and computer facilities without becoming “office associates” within the meaning of *R.* 1:15-5(b), but only after noting that “the material relating to individual cases of each attorney is maintained on separate ‘data’ disks used only by their respective secretaries and stored (while not in use) in each of their separate offices.” 111 *N.J.L.J.* 392 (April 14, 1983).

We stress that whenever attorneys enter into arrangement as outlined herein, the attorneys must exercise reasonable care to prevent the attorney's employees and associates, as well as others whose services are utilized by the attorney, from disclosing or using confidences or secrets of a client.

The attorneys should be particularly sensitive to this requirement and establish office procedures that will assure that confidences or secrets are maintained.

*Id.*

The critical requirement under *RPC* 1.6, therefore, is that the attorney “exercise reasonable care” against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access. “Reasonable care,” however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all

unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax.

What the term “reasonable care” means in a particular context is not capable of sweeping characterizations or broad pronouncements. But it certainly may be informed by the technology reasonably available at the time to secure data against unintentional disclosure. Obviously, in this area, changes in technology occur at a rapid pace. In 1983, for instance, when Opinion 515 was published, the personal computer was still somewhat of a novelty, and the individual floppy disk was the prevailing data storage device. The “state of the art” in maintaining electronic security was not very developed, but the ability to prevent unauthorized access by physically securing the floppy disk itself satisfied us that confidentiality could be maintained. By implication, at the time we were less accepting of data stored on a shared hard drive, even one that was partitioned to provide for individual private space for use by different firms, because of the risk of breach of confidentiality under prevailing technology.

We are of course aware that floppy disks have now become obsolete, and that it is exceedingly unlikely in this day and age that different law firms would attempt to share hard drive space on a conventional desktop computer, given the small cost of such computers in today’s market. New scenarios have arisen, however. It is very possible that a firm might seek to store client sensitive data on a larger file server or a web server provided by an outside Internet Service Provider (and shared with other clients of the ISP) in order to make such information available to clients, where access to that server may not be exclusively controlled by the firm’s own personnel. And in the context originally raised by the inquirer, it is almost always the case that a law firm will not have its own exclusive email network that reaches beyond its offices, and thus a document sent by email will very likely pass through an email provider that is not under the control of the attorney.

We are reluctant to render an specific interpretation of *RPC* 1.6 or impose a requirement that is tied to a specific understanding of technology that may very well be obsolete tomorrow. Thus, for instance, we do not read *RPC* 1.6 or Opinion 515 as imposing a per se requirement that, where data is available on a secure web server, the server must be subject to the exclusive command and control of the firm through its own employees, a rule that would categorically forbid use of an outside ISP. The very nature of the Internet makes the location of the physical equipment somewhat irrelevant, since it can be accessed remotely from any other Internet address. Such a requirement would work to the disadvantage of smaller firms for which such a dedicated IT staff is not practical, and deprive them and their clients of the potential advantages in enhanced communication as a result.

Moreover, it is not necessarily the case that safeguards against unauthorized disclosure are inherently stronger when a law firm uses its own staff to maintain a server. Providing security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry, and it is certainly possible that an independent ISP may more efficiently and effectively implement such security precautions.

We do think, however, that when client confidential information is entrusted in unprotected form, even temporarily, to someone outside the firm, it must be under a circumstance in which the outside party is aware of the lawyer's obligation of confidentiality, and is itself obligated, whether by contract, professional standards, or otherwise, to assist in preserving it. Lawyers typically use messengers, delivery services, document warehouses, or other outside vendors, in which physical custody of client sensitive documents is entrusted to them even though they are not employed by the firm. The touchstone in using "reasonable care" against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has

come to the prudent professional judgment he has satisfied both these criteria, then “reasonable care” will have been exercised.<sup>1</sup>

---

<sup>1</sup> In the specific context presented by the inquirer, where a document is transmitted to him by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access.

**ATTACHMENT M:**  
**New York**

## **Ethics Opinion 842**

### COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

**Topic:** Using an outside online storage provider to store client confidential information.

**Digest:** A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

**Rules:** 1.4, 1.6(a), 1.6(c)

#### QUESTION

**1. May a lawyer use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty? If so, what steps should the lawyer take to ensure that the information is sufficiently secure?**

#### OPINION

**2. Various companies offer online computer data storage systems that are maintained on an array of Internet servers located around the world. (The array of Internet servers that store the data is often called the "cloud.") A solo practitioner would like to use one of these online "cloud" computer data storage systems to store client confidential information. The lawyer's aim is to ensure that his clients' information will not be lost if something happens to the lawyer's own computers. The online data storage system is password-protected and the data stored in the online system is encrypted.**

**3. A discussion of confidential information implicates Rule 1.6 of the New York Rules of Professional Conduct (the "Rules"), the general rule governing confidentiality. Rule 1.6(a) provides as follows:**

**A lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of a lawyer or a third person, unless:**

- (1) the client gives informed consent, as defined in Rule 1.0(j);**
- (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or**
- (3) the disclosure is permitted by paragraph (b).**

4. The obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client's confidential information. *See* N.Y. County 733 (2004) (an attorney "must diligently preserve the client's confidences, whether reduced to digital format, paper, or otherwise"). As a New Jersey ethics committee observed, even when a lawyer wants a closed client file to be destroyed, "[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties." New Jersey Opinion (2006), *quoting* New Jersey Opinion 692 (2002).

5. In addition, Rule 1.6(c) provides that an attorney must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except to the extent disclosure is permitted by Rule 1.6(b). Accordingly, a lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney's supervision or who have been retained by the attorney to assist in providing services to the client. We note, however, that exercising "reasonable care" under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access.

6. To date, no New York ethics opinion has addressed the ethics of *storing* confidential information online. However, in N.Y. State 709 (1998) this Committee addressed the duty to preserve a client's confidential information when *transmitting* such information electronically. Opinion 709 concluded that lawyers may transmit confidential information by e-mail, but cautioned that "lawyers must always act reasonably in choosing to use e-mail for confidential communications." The Committee also warned that the exercise of reasonable care may differ from one case to the next. Accordingly, when a lawyer is on notice that the confidential information being transmitted is "of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail." *See also* Rule 1.6, cmt. 17 (a lawyer "must take reasonable precautions" to prevent information coming into the hands of unintended recipients when transmitting information relating to the representation, but is not required to use special security measures if the means of communicating provides a reasonable expectation of privacy).

7. Ethics advisory opinions in several other states have approved the use of electronic storage of client files provided that sufficient precautions are in place. *See, e.g.*, New Jersey Opinion 701 (2006) (lawyer may use electronic filing system whereby all documents are scanned into a digitized format and entrusted to someone outside the firm provided that the lawyer exercises "reasonable care," which includes entrusting documents to a third party with an enforceable obligation to preserve confidentiality and security, and employing available technology to guard against reasonably foreseeable attempts to infiltrate data); Arizona Opinion 05-04 (2005) (electronic storage of client files is permissible provided lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or

inadvertence"); *see also* Arizona Opinion 09-04 (2009) (lawyer may provide clients with an online file storage and retrieval system that clients may access, provided lawyer takes reasonable precautions to protect security and confidentiality and lawyer periodically reviews security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected).

8. Because the inquiring lawyer will use the online data storage system for the purpose of preserving client information - a purpose both related to the retention and necessary to providing legal services to the client - using the online system is consistent with conduct that this Committee has deemed ethically permissible. *See* N.Y. State 473 (1977) (absent client's objection, lawyer may provide confidential information to outside service agency for legitimate purposes relating to the representation provided that the lawyer exercises care in the selection of the agency and cautions the agency to keep the information confidential); *cf.* NY CPLR 4548 (privileged communication does not lose its privileged character solely because it is communicated by electronic means or because "persons necessary for the delivery or facilitation of such electronic communication may have access to" its contents).

9. We conclude that a lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of

his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. *See* Rule 1.4 (mandating communication with clients); *see also* N.Y. State 820 (2008) (addressing Web-based email services).

11. Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *See, e.g., City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619, 177 L.Ed.2d 216 (2010) (holding that City did not violate Fourth Amendment when it reviewed transcripts of messages sent and received by police officers on police department pagers); *Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. 2007) (e-mails between hospital employee and his personal attorneys were not privileged because employer's policy regarding computer use and e-mail monitoring stated that employees had no reasonable expectation of privacy in e-mails sent over the employer's e-mail server). *But see Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 990 A.2d 650 (2010) (despite employer's e-mail policy stating that company had right to review and disclose all information on "the company's media systems and services" and that e-mails were "not to be considered private or personal" to any employees, company violated employee's attorney-client privilege by reviewing e-mails sent to employee's personal attorney on employer's laptop through employee's personal, password-protected e-mail account).

12. This Committee's prior opinions have addressed the disclosure of confidential information in metadata and the perils of practicing law over the Internet. We have noted in those opinions that the duty to "exercise reasonable care" to prevent disclosure of confidential information "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks" in transmitting information electronically. N.Y. State 782 (2004), *citing* N.Y. State 709 (1998) (when conducting trademark practice over the Internet, lawyer had duty to "stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost"); *see also* N.Y. State 820 (2008) (same in context of using e-mail service provider that scans e-mails to generate computer advertising). The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.

## CONCLUSION

13. A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and

**the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.**

**(75-09)**

*One Elk Street, Albany, NY 12207*

*Phone: 518-463-3200 Secure Fax: 518.463.5993*

© 2014 New York State Bar Association

**ATTACHMENT N:**  
**North Carolina**

# 2011 Formal Ethics Opinion 6

January 27, 2012

## Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property

*Opinion rules that a lawyer may contract with a vendor of software as a service provided the lawyer uses reasonable care to safeguard confidential client information.*

### Inquiry #1:

Much of software development, including the specialized software used by lawyers for case or practice management, document management, and billing/financial management, is moving to the “software as a service” (SaaS) model. The American Bar Association’s Legal Technology Resource Center explains SaaS as follows:

SaaS is distinguished from traditional software in several ways. Rather than installing the software to your computer or the firm’s server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the internet. Data is stored in the vendor’s data center rather than on the firm’s computers. Upgrades and updates, both major and minor, are rolled out continuously...SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up front.<sup>1</sup>

Instances of SaaS software extend beyond the practice management sphere addressed above, and can include technologies as far-ranging as web-based email programs, online legal research software, online backup and storage, text messaging/SMS (short message service), voicemail on mobile or VoIP phones, online communication over social media, and beyond.

SaaS for law firms may involve the storage of a law firm’s data, including client files, billing information, and work product, on remote servers rather than on the law firm’s own computer and, therefore, outside the direct control of the firm’s lawyers. Lawyers have duties to safeguard confidential client information, including protecting that information from unauthorized disclosure, and to protect client property from destruction, degradation, or loss (whether from system failure, natural disaster, or dissolution of a vendor’s business). Lawyers also have a continuing need to retrieve client data in a form that is usable outside of a vendor’s product.<sup>2</sup> Given these duties and needs, may a law firm use SaaS?

### Opinion #1:

Yes, provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client’s file, from risk of loss.

The use of the internet to transmit and store client information presents significant challenges. In this complex and technical environment, a lawyer must be able to fulfill the fiduciary obligations to protect confidential client information and property from risk of disclosure and loss. The lawyer must protect against security weaknesses unique to the internet, particularly “end-user” vulnerabilities found in the lawyer’s own law office. The lawyer must also engage in periodic education about ever-changing security risks presented by the internet.

Rule 1.6 of the Rules of Professional Conduct states that a lawyer may not reveal information acquired during the professional relationship with a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation. Comment [17] explains, “A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.” Comment [18] adds that, when transmitting confidential client information, a lawyer must take “reasonable precautions to prevent the information from coming into the hands of unintended recipients.”

Rule 1.15 requires a lawyer to preserve client property, including information in a client’s file such as client documents and lawyer work product, from risk of loss due to destruction, degradation, or loss. *See also* RPC 209 (noting the “general fiduciary duty to safeguard the property of a client”), RPC 234 (requiring the storage of a client’s original documents with legal significance in a safe place or their return to the client), and 98 FEO 15 (requiring exercise of lawyer’s “due care” when selecting depository bank for trust account).

Although a lawyer has a professional obligation to protect confidential information from unauthorized disclosure, the Ethics Committee has long held that this duty does not compel any particular mode of handling confidential information nor does it prohibit the employment of vendors whose services may involve the handling of documents or data containing client information. *See* RPC 133 (stating there is no requirement that firm’s waste paper be shredded if lawyer ascertains that persons or entities responsible for the disposal employ procedures that

effectively minimize the risk of inadvertent or unauthorized disclosure of confidential information). Moreover, while the duty of confidentiality applies to lawyers who choose to use technology to communicate, "this obligation does not require that a lawyer use only infallibly secure methods of communication." RPC 215. Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise affected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality. *Id.*

Furthermore, in 2008 FEO 5, the committee held that the use of a web-based document management system that allows both the law firm and the client access to the client's file is permissible:

provided the lawyer can fulfill his obligation to protect the confidential information of all clients. A lawyer must take steps to minimize the risk that confidential client information will be disclosed to other clients or to third parties. See RPC 133 and RPC 215.... A security code access procedure that only allows a client to access its own confidential information would be an appropriate measure to protect confidential client information.... If the law firm will be contracting with a third party to maintain the web-based management system, the law firm must ensure that the third party also employs measures which effectively minimize the risk that confidential information might be lost or disclosed. See RPC 133.

In a recent ethics opinion, the Arizona State Bar's Committee on the Rules of Professional Conduct concurred with the interpretation set forth in North Carolina's 2008 FEO 5 by holding that an Arizona law firm may use an online file storage and retrieval system that allows clients to access their files over the internet provided the firm takes reasonable precautions to protect the security and confidentiality of client documents and information.<sup>3</sup>

In light of the above, the Ethics Committee concludes that a law firm may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.

No opinion is expressed on the business question of whether SaaS is suitable for a particular law firm.

#### **Inquiry #2:**

Are there measures that a lawyer or law firm should consider when assessing a SaaS vendor or seeking to minimize the security risks of SaaS?

#### **Opinion #2:**

This opinion does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required.

Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer. The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security. Some recommended security measures are listed below.

- Inclusion in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.
- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
- Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.
- Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.<sup>4</sup>
- Evaluation of the extent to which the SaaS vendor backs up hosted data.

## Endnotes

1. FYI: Software as a Service (SaaS) for Lawyers, ABA Legal Technology Resource Center at [abanet.org/tech/ltrc/fyidocs/saas.html](http://abanet.org/tech/ltrc/fyidocs/saas.html).

2. *Id.*

3. Paraphrasing the description of a lawyer's duties in Arizona State Bar Committee on Rules of Professional Conduct, Opinion 09-04 (Dec. 9, 2009).

4. A firewall is a system (which may consist of hardware, software, or both) that protects the resources of a private network from users of other networks. Encryption techniques are methods for ciphering messages into a foreign format that can only be deciphered using keys and reverse encryption algorithms. A socket security feature is a commonly-used protocol for managing the security of message transmission on the internet. An intrusion detection system is a system (which may consist of hardware, software, or both) that monitors network and/or system activities for malicious activities and produces reports for management.

---

## **THE NORTH CAROLINA STATE BAR**

217 E. Edenton Street • PO Box 25908 • Raleigh, NC 27611-5908 • 919.828.4620

Copyright © North Carolina State Bar. All rights reserved.

**ATTACHMENT 0:**  
**Ohio**

July 25, 2013

**Re: Request for Informal Advisory Opinion**

Dear \_\_\_\_\_:

You have requested the opinion of the Ohio State Bar Association Professionalism Committee on whether your law firm may use a third-party vendor to store client data in “the cloud.” As you describe it, your firm currently backs up its computer files, including client documents and data, on a server located on site. You are considering a third-party vendor that is offering a program that would use “a major software provider to securely store your data off site,” which your law firm would be able to access via the Internet. You indicate that the data would be encrypted before it left the law firm and would remain encrypted at the offsite data center, located in Atlanta.

The Committee’s opinion is that storing client data in “the cloud” is a permutation on traditional ways of storing client data, and requires lawyers to follow the ethics rules that apply to client information in whatever form. With due regard for these rules and related Ohio ethics opinions, the Committee advises that the Ohio Rules of Professional Conduct do not prohibit storing client data in “the cloud.”

**Applicable Rules of Professional Conduct:**

Your request for an opinion requires consideration of the following provision of the Ohio Rules of Professional Conduct (“ORPC” or “Rules”):

- 1.1 (lawyer shall provide competent representation);
- 1.4(a)(2) (lawyer shall reasonably consult with client about means by which client’s objectives are to be accomplished);
- 1.6(a) (lawyer shall preserve confidentiality of information relating to the representation, subject to certain limited exceptions);
- 1.15(a) (lawyer shall safeguard client property);
- 5.3(a)-(b) (with respect to a non-lawyer employed by, retained by or associated with a lawyer, lawyer shall make reasonable efforts to ensure that the non-lawyer’s conduct is compatible with lawyer’s professional obligations).

## Opinion:

The “cloud” is “merely ‘a fancy way of saying stuff’s not on your [own] computer.’” Formal Op. 2011-200, 1 (Pa. Bar Ass’n. Comm. on Legal Ethics & Prof’l Respon. 2011). More formally, cloud storage is the use of “internet-based computing in which large groups of remote servers are networked so as to allow ... centralized data storage.” Andrew L. Askew, *iEthics: How Cloud Computing has Impacted the Rules of Professional Conduct*, 88 N. Dak. L. Rev. 453, 457 (2012).

Due to “recent advances in ... technology, the ways attorneys are able to perform and deliver legal services have drastically changed.” Askew, *supra* at 466. The applicable Ohio Rules of Professional Conduct, however, are adaptable to address new technologies. Regarding cloud storage, the key rules are those relating to competent representation, communicating with the client, preserving client confidentiality, safeguarding the client’s property and supervising non-lawyers that provide support services. The obligations expressed in these rules operate as they traditionally have for older data storage methods. *See, e.g.*, Adv. Op. 99-2 (Ohio Bd. of Comm’rs on Grievances & Disc. Apr. 9, 1999) (communicating by e-mail was not contemplated in 1970, when former disciplinary rule on confidentiality was adopted by Ohio Supreme Court, but “nevertheless, the rule applies” to e-mail).

The issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices. The analogy to paper files can help lawyers as they exercise their professional judgment in adopting specific practices that address new storage technologies such as “the cloud.” That process of exercising individual judgment would not be assisted by overly-detailed regulatory input from this Committee. As one state bar ethics committee noted, a lawyer “has always been under a duty to make reasonable judgments when protecting client property and information. *Specific practices regarding protection of client property and information have always been left up to individual lawyers’ judgment, and that same approach applies to the use of online data storage,*” subject as always to the relevant conduct rules. Adv. Op. 2215, 2 (Wash. St. Bar Rules of Prof’l Cond. Comm. 2012) (emphasis added).

This approach – applying existing principles to new technological advances while refraining from mandating specific practices – is a practical one. Because technology changes so quickly, overly-specific rules would become obsolete as soon as they were issued. *See* Ethics Op. 2010-6 (Vt. Bar Prof’l Respon. Section 2010) (dynamism of cloud computing makes it unwise to establish “specific conditions precedent” to use). For example, rules about exactly what security measures are required in order to protect client data stored in the cloud would be superseded quickly by technological advances.<sup>1</sup>

---

<sup>1</sup> The American Bar Association’s recent promulgation through the Commission on Ethics 20/20 of rule changes and new comments for the Model Rules of Professional Conduct (“MRPC”) is in line with this approach. The Commission on Ethics 20/20 proposed and the ABA House of Delegates adopted minor changes to existing rules rather than specific regulations aimed at specific new technologies. *See e.g.*, revised cmt. [8] to MRPC 1.1 (lawyer should keep

Against that background, there are four main issues to consider in applying the Ohio Rules of Professional Conduct to cloud storage of client data: competently selecting an appropriate vendor; preserving confidentiality and safeguarding the client's data; supervising cloud storage vendors; and communicating with the client

1. *Competently selecting an appropriate vendor for cloud storage*

The duty of competence under ORPC 1.1 requires a lawyer to exercise the “legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.” In Ohio Advisory Opinion 2009-6 (Aug. 14, 2009), the Ohio Board of Commissioners on Grievances and Discipline (“Board”) opined that a lawyer who selects a vendor for *any* type of support services that are provided outside the lawyer’s firm must exercise “due diligence as to the qualifications and reputation of those to whom services are outsourced,” and also as to whether the outside vendor will itself provide the requested services competently and diligently. *Id.* at 6.<sup>2</sup>

Knowing the qualifications, reputation and longevity of your cloud storage vendor is necessary. But in addition, just as you would review and assess the terms of a contract for off-site storage of your clients’ paper files in a brick-and-mortar facility, so you must read and under-

---

up with changes in law and its practice, “including the benefits and risks associated with relevant technology”) (emphasis added); new cmt. [3] to MRPC 5.3 (lawyer may use outside non-lawyers to assist in rendering legal services; “[e]xamples include ... using an Internet-based service to store client information.”; extent of lawyer’s obligation to ensure that non-lawyers provide services in a manner compatible with lawyer’s professional obligations “will depend upon the circumstances.”) (emphasis added).

Ohio has not yet adopted any of the revised provisions of the Model Rules. See Univ. of Akron Miller-Becker Ctr. for Prof’l Respon., *Navigating the Practice of Law in the Wake of Ethics 20/20 - Globalization, New Technologies, and What It Means to be a Lawyer in these Uncertain Times* (Apr. 4-5, 2013), available at <http://tinyurl.com/lblj6q8> (examining Ethics 20/20’s final work and its impact in Ohio and elsewhere); Frank E. Quirk, *Lawyer Ethics for the 21st Century*, 19-21 Ohio Lawyer (Jan. - Feb. 2013) (discussing Ethics 20/20, including possible future impact on ORPC).

<sup>2</sup> Lawyers can call on many resources to assist in selecting a vendor. See, e.g., John Edwards, *How to Pick the Best Cloud*, Law Technology News (June 11, 2013), available at <http://tinyurl.com/k77w2sg>; Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing*, ABA Section of Litigation (Feb. 7, 2013), available at <http://tinyurl.com/ksaeww8>; Am. Bar Ass’n, *Moving Your Law Practice to the Cloud Safely and Ethically* (Jan. 14, 2013), available at <http://tinyurl.com/kr3s2xw>; Am. Bar Ass’n, *Evaluating Cloud-Computing Providers* (YourABA June 2012), available at <http://tinyurl.com/l7b9wfh>. See generally, Nick Pournader, *Embracing Technology’s ‘Cloudy’ Frontier*, Law Practice Today (webzine of ABA Law Practice Management Section) (Oct. 2010), available at <http://tinyurl.com/k54f3gh>.

stand the agreement you enter into with an online data storage service – sometimes called a “Service Level Agreement.”<sup>3</sup> Some commonly-occurring issues include:

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor’s part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give “ownership” of the data to the vendor, or is the data merely subject to the vendor’s license?<sup>4</sup>
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor’s policy regarding returning your client data at the termination of its relationship with your firm?
- What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?
- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

## 2. *Preserving confidentiality and safeguarding client property*

Under ORPC 1.6(a), a lawyer “shall not reveal information relating to the representation of a client,” with only limited exceptions. As recommended by the Commission on Ethics 20/20, the ABA House of Delegates added Model Rule 1.6(c) in August 2012, requiring a lawyer to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” The Ohio Supreme Court has not considered or adopted that change. Yet the language of the new Model Rule only makes explicit a duty that is already implicit in Ohio’s current Rule 1.6(a). That duty is to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in.

---

<sup>3</sup> See Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?*, Slaw (Canadian online legal magazine) (Jan. 30, 2012), available at <http://tinyurl.com/m425p3j> (discussing Apple iCloud terms and conditions of use and expressing doubt that attorneys have read them).

<sup>4</sup> See § 2, below. A Service Level Agreement or terms of service that provide that the vendor “owns” the data would violate ORPC 1.15(a), which requires that client property “be identified as such” and “appropriately safeguarded.”

For instance, in Advisory Opinion 99-2 (Apr. 9, 1999), the Board said that communicating with clients by e-mail was covered by the confidentiality rule in the former Code of Professional Responsibility, which “establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty extends to communications by electronic methods just as it extends to other forms of communication used by an attorney.” *Id.* at 3. Significantly, the Board ruled that it was not necessary to encrypt e-mail communications with clients, despite the possibility that such communications might be electronically intercepted. Such a risk was not unique to e-mail in the Board’s view, and did not call for extraordinary methods of protection:

Every method of communication carries with it a risk of interception. Mail can be intercepted. Telephone messages can also be intercepted. Land-based telephones may be wiretapped, eavesdropping may occur by listening through a receiver of a telephone extension, or too loud voices may be overheard by others. Yet, these forms of communication are considered reasonable under the rule. .... To summarize, additional security measures, such as scrambling devices or encoding methods, have not traditionally been required under [the confidentiality rule] for other forms of communication frequently used by attorneys, even though the communication may be susceptible of interception.

*Id.* at 9-10.

Rather, the Board emphasized that “an attorney must use his or her professional judgment to determine the appropriate method of each attorney-client communication,” and that client preference or particular specialized circumstances may call for taking additional measures to ensure confidentiality. *Id.* at 10-11.

In the same way, storing client data in the cloud involves yielding exclusive control over the information and puts it in the hands of a third party, just as storing a client’s paper files off-site does. And similar to storing a client’s paper files off-site, cloud storage raises the risk that “a third party could illegally gain access to ... confidential client data.” Formal Ethics Op. 2010-02, 14 (Ala. Disc. Comm. 2010). “[J]ust as with traditional storage and retention of client files, a lawyer cannot guarantee that client confidentiality will never be breached, whether by an employee or some other third-party.” *Id.* at 15. Therefore, a lawyer’s duty under the ORPC to preserve the confidentiality of cloud-stored client data is to exercise competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data.

In the context of cloud storage, the requirement under ORPC 1.15(a) that client property “be identified as such and appropriately safeguarded” is a corollary to the duty to preserve the confidentiality of information related to the representation. A client’s information and documents in whatever form can be construed as its “property” when in the lawyer’s possession. Safeguarding such property includes reasonably ensuring that the vendor has systems in place to

protect client data from destruction, loss or unavailability. In addition, terms of service that provide or suggest that the cloud storage vendor acquires an ownership interest in the electronic data on its servers would violate the duty to keep client property “identified as such.”

### 3. *Supervising cloud vendors*

Rule 5.3(a) of the ORPC requires that law firms make reasonable efforts to have policies and procedures in place that give reasonable assurance that the conduct of a non-lawyer employed by the lawyer is “compatible with the professional obligations of the lawyer.” And under Rule 5.3(b), individual lawyers who have supervisory authority over non-lawyers must likewise make reasonable efforts to ensure that the non-lawyer’s conduct is compatible with the lawyers’ own professional obligations.

In its Advisory Opinion 2009-6, *supra*, the Board explained how these duties apply when lawyers outsource non-legal “support services,” defined to encompass all varieties of “ministerial” services that are non-legal in nature. *Id.* at 3. The Board emphasized that while Rule 5.3’s supervisory duties apply to lawyers when they outsource to support-service vendors, “the *extent* of supervision for outsourced services is a matter of professional judgment for an Ohio lawyer,” subject to the requirement that lawyers exercise that judgment with the diligence due under the Rules – particularly as to the vendor’s qualifications, competence and ability to protect confidentiality. *Id.* at 8 (emphasis added).

Storing client data in “the cloud” is almost by definition a service that lawyers will outsource, and cloud-storage vendors provide the kind of “ministerial” non-legal support services that are contemplated under the Board’s Advisory Opinion 2009-6. Therefore, under Rule 5.3(a)-(b), lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor’s conduct is compatible with the lawyer’s own professional obligations. While the extent of supervision needed is a matter of professional judgment for the lawyer, the lawyer must exercise due diligence in ascertaining whether the vendor will be capable of conduct consistent with the lawyer’s own obligations.

### 4. *Communicating with the client*

Rule 1.4(a)(2) requires a lawyer to “reasonably consult with the client” about how the client’s objectives are to be accomplished. We do not conclude that storing client data in “the cloud” always requires prior client consultation, because we interpret the language “reasonably consult” as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation. Our opinion on this point is in line with ethics authorities in other jurisdictions that have considered the question. *See, e.g.*, Formal Op. 2011-200, 5-6 (Pa. Bar Ass’n Comm. on Legal Ethics & Prof’l Respon. 2011) (not necessary to “communicate every minute detail” of representation, but it may at times be necessary to inform client of lawyer’s use of cloud computing, depending on scope of representation and sensitivity of data involved); Adv. Op. 2012-13/4 (N.H. Bar Ass’n Ethics Comm. 2012) (where highly sensitive data involved, “may become necessary” to inform client and obtain consent for lawyer’s use of cloud computing). In exercising judgment about whether to consult with the client about storing client data in “the cloud,” the lawyer should consider, among other things, the sensitivity of the client’s data.

5. *Ethics opinions from other jurisdictions regarding cloud storage*

Our conclusion that cloud storage is permissible under the ORPC is echoed by ethics authorities in other jurisdictions. To date, at least 14 states have issued ethics opinions regarding or related to cloud data storage. All have concluded that their respective lawyer conduct rules permit lawyers to store client data in the cloud, with due regard for their state ethics rules, usually their states' versions of ORPC 1.1, 1.6, 1.15 and 5.3.<sup>5</sup>

**Conclusion:**

Storing client data in “the cloud” can provide benefits to lawyers and clients by facilitating access to client data, increasing efficiency and reducing the cost of legal services. The Ohio Rules of Professional Conduct do not prohibit cloud storage, provided that lawyers follow the ethics rules that apply to client information in whatever form and are guided by applicable Ohio ethics opinions.

Sincerely,

Professionalism Committee  
OHIO STATE BAR ASSOCIATION

**Note: Advisory Opinions of the Ohio State Bar Association Professionalism Committee are informal, non-binding opinions in response to prospective or hypothetical questions regarding the application of the Supreme Court Rules for the Government of the Judiciary, the Rules of Professional Conduct, the Code of Judicial Conduct, and the Attorney's Oath of Office.**

---

<sup>5</sup> The ABA has summarized and charted the opinions on cloud ethics issues via the ABA's Law Practice Management Section's Legal Technology Resource Center. See Am. Bar Ass'n, *Cloud Ethics Opinions Around the U.S.*, available at <http://tinyurl.com/733gyr8>.

**ATTACHMENT P:**  
**Oregon**

## FORMAL OPINION NO. 2011-188

### Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials

#### Facts:

Law Firm contracts with third-party vendor to store client files and documents online on remote server so that Lawyer and/or Client could access the documents over the Internet from any remote location.

#### Question:

May Lawyer do so?

#### Conclusion:

Yes, qualified.

#### Discussion:

With certain limited exceptions, the Oregon Rules of Professional Responsibility require a lawyer to keep client information confidential. *See* Oregon RPC 1.6.<sup>1</sup> In addition, Oregon RPC 5.3 provides:

---

<sup>1</sup> Oregon RPC 1.6 provides:

- (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
- (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
  - (1) to disclose the intention of the lawyer's client to commit a crime and the information necessary to prevent the crime;
  - (2) to prevent reasonably certain death or substantial bodily harm;
  - (3) to secure legal advice about the lawyer's compliance with these Rules;
  - (4) to establish a claim or defense on behalf of the lawyer in controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;
  - (5) to comply with other law, court order, or as permitted by these Rules; or

With respect to a nonlawyer employed or retained, supervised or directed by a lawyer:

- (a) a lawyer having direct supervisor authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
- (b) except as provided by Rule 8.4(b), a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by the nonlawyer if:
  - (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
  - (2) the lawyer is a partner or has comparable managerial authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Lawyer may store client materials on a third-party server so long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation.<sup>2</sup> To do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential. Under certain circumstances, this may be satisfied through a third-party vendor's compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the Lawyer by the Oregon RPCs. This may include, among other things, ensuring the service agreement requires the vendor to preserve the confidentiality and security of the materials. It may also require that

- 
- (6) to provide the following information in discussions preliminary to the sale of a law practice under Rule 1.17 with respect to each client potentially subject to the transfer: the client's identity; the identities of any adverse parties the nature and extent of the legal services involved; and fee and payment information. A potential purchasing lawyer shall have the same responsibilities as the lawyer to preserve confidences and secrets of such clients whether or not the sale of the practice closes or the client ultimately consents to representation by the purchasing lawyer.

<sup>2</sup> Some call the factual scenario presented above "cloud computing." See Richard Acello, *Get Your Head in the Cloud*, ABA Journal, April 2010, at 28–29 (providing that "cloud computing" is a "sophisticated form of remote electronic data storage on the internet" and "[u]nlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored 'in the cloud' is kept on large servers located elsewhere and maintained by a vendor").

vendor notify Lawyer of any nonauthorized third-party access to the materials. Lawyer should also investigate how the vendor backs up and stores its data and metadata to ensure compliance with the Lawyer's duties.<sup>3</sup>

Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology "available at the time to secure data against unintentional disclosure."<sup>4</sup> As technology advances, the third-party vendor's protective measures may become less secure or obsolete over time.<sup>5</sup> Accordingly, Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials.<sup>6</sup>

**Approved by Board of Governors, November 2011.**

---

<sup>3</sup> See OSB Formal Ethics Op No 2005-141, which provides: "As long as Law Firm makes reasonable efforts to ensure that recycling company's conduct is compatible with Law Firm's obligation to protect client information, the proposed conduct is permissible. Reasonable efforts include, at least, instructing the recycling company about Law Firm's duties pursuant to Oregon RPC 1.6 and obtaining its agreement to treat all materials appropriately." *See also* OSB Formal Ethics Op Nos 2005-129, 2005-44.

<sup>4</sup> *See* NJ Ethics Op 701 (discussing electronic storage and access to files).

<sup>5</sup> *See* Arizona Ethics Op 09-04 (discussing confidentiality, maintaining client files, electronic storage, and the Internet).

<sup>6</sup> A lawyer's obligation in the event of a breach of security of confidential materials is outside the scope of this opinion.

**ATTACHMENT Q:**  
**Pennsylvania**



**PENNSYLVANIA BAR ASSOCIATION COMMITTEE ON LEGAL ETHICS AND  
PROFESSIONAL RESPONSIBILITY**

**ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/  
SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF  
CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY**

**FORMAL OPINION 2011-200**

**I. Introduction and Summary**

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using “cloud computing.” While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely “a fancy way of saying stuff’s not on your computer.”<sup>1</sup>

From a more technical perspective, “cloud computing” encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service (“SaaS”), platform-as-a-service (“PaaS”), infrastructure-as-a-service (“IaaS”), Amazon Elastic Cloud Compute (“Amazon EC2”), and Google Docs.

This opinion places all such software and services under the “cloud computing” label, as each raises essentially the same ethical issues. In particular, the central question posed by “cloud computing” may be summarized as follows:

May an attorney ethically store confidential client material in “the cloud”?

In response to this question, this Committee concludes:

Yes. An attorney may ethically allow client confidential material to be stored in “the cloud” provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

\*\*\*\*\*

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

---

<sup>1</sup> Quinn Norton, “Byte Rights,” *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than “cloud computing,” which refers to software and related services that store information on a remote computer, *i.e.*, a computer or server that is not located at the law office’s physical location. Rather, the information is stored on another company’s server, or many servers, possibly all over the world, and the user’s computer becomes just a way of accessing the information.<sup>2</sup>

The advent of “cloud computing,” as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in “cloud computing.”

Recent “cloud” data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission (“FTC”) has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of “cloud computing” and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations (“FBI”) warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms’ databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 (“Metadata”) and 2010-200 (“Virtual Law Offices”), and an informal Opinion directly addressing “cloud computing.” Because of the importance of “cloud computing” to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing “cloud computing.”

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.*, products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

## **II. Background**

For lawyers, “cloud computing” may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with “cloud computing,” an attorney can simplify document management and control costs.

---

<sup>2</sup> *Id.*

The benefits of using “cloud computing” may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because “cloud computing” refers to “offsite” storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

### **III. Discussion**

#### **A. Prior Pennsylvania Opinions**

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office “is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office.” Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on “cloud computing” stated that an attorney may ethically allow client confidential material to be stored in “the cloud” provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

## **B. Pennsylvania Rules of Professional Conduct**

An attorney using “cloud computing” is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses “cloud computing,” the following rules, *inter alia*, are implicated:

Rule 1.0 (“Terminology”);  
Rule 1.1 (“Competence”);  
Rule 1.4 (“Communication”);  
Rule 1.6 (“Confidentiality of Information”);  
Rule 1.15 (“Safekeeping Property”); and  
Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistants”).

Rule 1.1 (“Competence”) states:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [5] (“Thoroughness and Preparation”) of Rule 1.1 provides further guidance about an attorney’s obligations to clients that extend beyond legal skills:

Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. ...

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney’s “methods and procedures.” Part of a lawyer’s responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like “cloud computing,” require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in “cloud computing” is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children’s show “Zodiac Island” lost an entire season’s worth of episodes when a fired employee for the show’s data hosting service accessed the show’s content without authorization and wiped it out.<sup>3</sup>

---

<sup>3</sup> Eriq Gardner, “Hacker Erased a Season’s Worth of ‘Zodiac Island’,” *Yahoo! TV* (March 31, 2011), available at [http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us\\_zodiac](http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac)

Rule 1.15 (“Safekeeping Property”) requires that client property should be “appropriately safeguarded.”<sup>4</sup> Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

(b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer’s own property. Such property shall be identified and appropriately safeguarded.

Rule 1.6 (“Confidentiality of Information”) states in relevant part:

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

(d) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

A fundamental principle in the client-lawyer relationship is that, in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. ...

Also relevant is Rule 1.0(e) defining the requisite “Informed Consent”:

“Informed consent” denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client’s informed consent is required. While it is not necessary to communicate every minute

---

<sup>4</sup> In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the “cloud.”

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).<sup>5</sup> This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

---

<sup>5</sup> The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using “cloud computing” services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.<sup>6</sup>

Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistants”) states:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) A partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person’s conduct is compatible with the professional obligations of the lawyer.

(b) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer; and

(c) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

At its essence, “cloud computing” can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client’s interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client’s matter.

### **C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider**

---

<sup>6</sup> Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of “cloud computing,” an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney’s direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. Competency extends beyond protecting client information and confidentiality; it also includes a lawyer’s ability to reliably access and provide information relevant to a client’s case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider. However, since cloud services are under the provider’s control, using “the cloud” to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for “cloud computing” may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm’s network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
- Ensuring the provider:
  - explicitly agrees that it has no ownership or security interest in the data;
  - has an enforceable obligation to preserve security;
  - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
  - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
  - includes in its “Terms of Service” or “Service Level Agreement” an agreement about how confidential client information will be handled;
  - provides the firm with right to audit the provider’s security procedures and to obtain copies of any security audits performed;
  - 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;
  - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
  - provides the ability for the law firm to get data “off” of the vendor’s or third party data hosting company’s servers for the firm’s own use or in-house backup offline.
- Investigating the provider’s:
  - security measures, policies and recovery methods;
  - system for backing up data;
  - security of data centers and whether the storage is in multiple centers;
  - safeguards against disasters, including different server locations;
  - history, including how long the provider has been in business;
  - funding and stability;
  - policies for data retrieval upon termination of the relationship and any related charges; and,
  - process to comply with data that is subject to a litigation hold.
- Determining whether:
  - data is in non-proprietary format;
  - the Service Level Agreement clearly states that the attorney owns the data;
  - there is a 3rd party audit of security; and,
  - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.
- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.<sup>7</sup>
- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the “cloud computing” services are offered, *i.e.*, Service Level Agreements (“SLAs”), may also present obstacles to reasonable care efforts. Most SLAs are essentially “take it or leave it,”<sup>8</sup> and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the “cloud computing” field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.<sup>9</sup>

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania’s notification law, 73 P.S. § 2303 (2011) (“Notification of Breach”), states:

(a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

---

<sup>7</sup> This is recommended even though many vendors will claim that it is not necessary.

<sup>8</sup> Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

<sup>9</sup> One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

(c) **VENDOR NOTIFICATION.** -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for “cloud computing.” In the survey, a number of the nearly 900 internet experts surveyed agreed that it “presents security problems and further exposes private information,” and some experts even predicted that “the cloud” will eventually have a massive breach from cyber-attacks.<sup>10</sup> Incident response plans should be in place before attorneys move to “the cloud”, and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be “private clouds.” Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

#### **D. Web-based E-mail**

Web-based email (“webmail”) is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of “cloud computing,” are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney’s obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, “Legal Ethics in the Cloud: Avoiding the Storms,” explains:

Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

---

<sup>10</sup> Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, <http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all>

these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.<sup>11</sup>

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.

It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.<sup>12</sup>

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) (“Transmission of Confidential Information by Electronic Mail”), which concluded that, “In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.”

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 (“Confidentiality of Information”).

Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate’s law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm’s mail room if that message contained client confidential

---

<sup>11</sup> David G. Ries, Esquire, “Legal Ethics in the Cloud: Avoiding the Storms,” course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).

<sup>12</sup> *Id.*

information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.

By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

#### **E. Opinions From Other Ethics Committees**

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while “cloud computing” is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.*, web-based email) and these conclusions are consistent with opinions about emergent emergent “cloud computing” technologies.

**The American Bar Association Standing Committee on Ethics and Professional Responsibility** has not yet issued a formal opinion on “cloud computing.” However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an “Issues Paper Concerning Client Confidentiality and Lawyers’ Use of Technology” (Sept. 20, 2010) and considered some of the concerns and ethical implications of using “the cloud.” The Working Group found that potential confidentiality problems involved with “cloud computing” include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

*Id.* The Working Group also stated, “[f]orms of technology other than ‘cloud computing’ can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen.” *Id.* Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

*Id.* Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 (“Terminology”), Model Rule 1.1 (“Competence”), and Model Rule 1.6 (“Duty of Confidentiality”) to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

Rule 1.1 (“Competence”) Comment [6] (“Maintaining Competence”): “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

Rule 1.6(c) (“Duty of Confidentiality”): “A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client.”

Rule 1.6 (“Duty of Confidentiality”) Comment [16] (“Acting Competently to Preserve Confidentiality”): “Paragraph (c) requires a ~~A~~ lawyer ~~must to~~ act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer’s supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id.*

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

**The Alabama State Bar** Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

**State Bar of Arizona** Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id.* Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

**The California State Bar** Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

**The Florida Bar** Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id.*

**Illinois State Bar** Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."<sup>13</sup>

**The Maine** Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id.*

Of note, the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provide a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

The contract between a covered entity and a business associate must provide that the business associate will:

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

---

<sup>13</sup> Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at <http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/>

- (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- (C) Report to the covered entity any security incident of which it becomes aware;
- (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

**Massachusetts Bar Association Ethics Opinion 05-04** (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id.*

**The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility** issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id.* Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

**The New Jersey State Bar Association Advisory Committee on Professional Ethics** issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id.* Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id.* The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

**The New York State Bar Association Committee on Professional Ethics** concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against “reasonably foreseeable” data infiltration by using available technology. *Id.*

**The North Carolina State Bar** Ethics Committee has addressed the issue of “cloud computing” directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that “a law firm may use SaaS<sup>14</sup> if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files.” *Id.* The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers “must protect against security weaknesses unique to the Internet, particularly ‘end-user’ vulnerabilities found in the lawyer’s own law office.” *Id.*

The Committee’s minimum requirements for reasonable care in Proposed Formal Opinion 6 included:<sup>15</sup>

- An agreement on how confidential client information will be handled in keeping with the lawyer’s professional responsibilities must be included in the SaaS vendor’s Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor’s data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;
- The agreement with the vendor must specify that firm’s data will be hosted only within a specified geographic area. If by agreement the data is 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 the state of North Carolina;
- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor’s software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

---

<sup>14</sup> SaaS, as stated above, stands for Software-as-a-Service and is a type of “cloud computing.”

<sup>15</sup> The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, “due diligence and perpetual education as to the security risks of SaaS are required.” Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data “off” the vendor’s or third party data hosting company’s servers for lawyers’ own use or in-house backup offline; and,
- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

**Vermont Bar Association** Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

**Virginia State Bar** Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)<sup>16</sup>, requiring “due care” in selecting the service provider and keeping the information confidential. *Id.*

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

#### **IV. Conclusion**

The use of “cloud computing,” and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

---

<sup>16</sup> Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

To the extent a lawyer reasonably believes necessary, the lawyer may reveal:

(6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in “the cloud.” Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using “cloud” software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.

**CAVEAT:** THE FOREGOING OPINION IS ADVISORY ONLY AND IS NOT BINDING ON THE DISCIPLINARY BOARD OF THE SUPREME COURT OF PENNSYLVANIA OR ANY COURT. THIS OPINION CARRIES ONLY SUCH WEIGHT AS AN APPROPRIATE REVIEWING AUTHORITY MAY CHOOSE TO GIVE IT.

**ATTACHMENT R:**  
**Vermont**

## OPINION 2010-6

### DIGEST:

Vermont attorneys can utilize Software as a Service in connection with confidential client information, property, and communications, including for storage, processing, transmission, and calendaring of such materials, as long as they take reasonable precautions to protect the confidentiality of and to ensure access to these materials.

### QUESTIONS PRESENTED

The Vermont Bar Association Professional Responsibility Section has been asked to address the propriety of use by attorneys and law firms of Software as a Service (“SaaS”) which is also known as Cloud Computing. Subsidiary questions include whether client documents and information can be remotely stored and backed up using SaaS systems; whether there is any subset of client property that cannot be stored using SaaS; whether lawyers can use SaaS and web-based email and calendaring systems; and whether use of remote document synchronization systems is permissible.

### RELEVANT RULES

#### Rule 1.6. Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . .

#### Comments to Rule 1.6: Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

#### Rule 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Rule 1.15. Safekeeping Property

(a)(1) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . . [Client] property shall be identified as such and appropriately safeguarded.

Rule 5.3. Responsibilities Regarding Nonlawyer Assistants

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer . . .

DISCUSSION

SaaS and Cloud Computing refer to a constellation of web-based data processing, transmission, and storage services that are available over the internet. In the past, client property was handled and stored on site, and lawyer-client communications occurred in person. Technological advances, however, have changed the way data is transmitted and stored, and the ways lawyers communicate with clients. These changes in technology have been accompanied by new questions about how lawyers should act to protect confidentiality of client information.

The propriety of lawyers using SaaS has attracted significant attention from Bar Association Ethics Committees in recent years, and a consensus position has been developing that allows lawyers to store client data in web based systems, and about the steps lawyers should consider and take when engaging in Cloud Computing. This opinion therefore now turns to a summary of recent ethics decisions addressing SaaS.

North Carolina Proposed Formal Ethics Opinion No. 6

Over a period spanning approximately 1½ years, the North Carolina State Bar Association has issued successive drafts of a formal ethics opinion addressing attorney use of SaaS. The third draft of this Formal Ethics Opinion, issued in October 2011, endorses the use of SaaS to store law firm data, including confidential client information, as long as steps are taken to protect the confidentiality of client information and to preserve client property. Proposed NC FEO 6 steps back from a series of mandatory steps that lawyers would have been required to take in connection with use of SaaS, as set forth in the previous April 2011 draft of this Opinion. Instead, the Opinion now provides that lawyers:

"may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect client information and to safeguard client

files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.”

Because of the rapidly changing nature of technology, Proposed NC FEO 6 declines to impose specific requirements on lawyers who use Cloud Computing in connection with client data. Instead, the Opinion identifies a series of steps that lawyers should consider taking before using SaaS, and requires lawyers to engage in ongoing due diligence and continuing legal education to ensure that remotely stored client data remains secure and accessible. Factors identified in this Opinion for those who use SaaS include:

- a. Understanding and protecting against security risks inherent in the internet, including end-user vulnerabilities in the lawyer’s office;
- b. Including provisions about protection of client confidences in the agreement between the lawyer and the SaaS vendor;
- c. Ensuring that there are mechanisms for obtaining access to, retrieving, and protecting data if the lawyer terminates use of the SaaS product, or if the SaaS vendor goes out of business or experiences a break in continuity;
- d. Carefully reviewing the terms of the user agreement, including its security provisions;
- e. Evaluating the security measures used by the vendor; and
- f. Confirming the extent to which the SaaS vendor backs up the data it is storing.

#### Iowa State Bar Association Ethics & Practice Committee Opinion 11-01

In September 2011, the Iowa State Bar Ethics and Practice Committee took a similar approach to Cloud Computing in Opinion 11-01. Applying comment 17 to Rule 1.6, Opinion

11-01 recognized that:

“the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.”

The Opinion declines to address in detail the specifics of individual SaaS products, because such guidance would quickly prove outdated, and may be beyond the scope of a lawyer’s expertise. Instead, Opinion 11-01 suggests a series of matters into which lawyers should inquire before storing client data on remote servers they do not control, including:

- a. Availability of unrestricted access to the data, and ability to access the data through alternate means;
- b. Performance of due diligence about the SaaS vendor, including its operating record, recommendations by other users, the provider’s operating location, its end user agreement (including provisions on choice of law, limitations on liability and damages, and rights in the stored data);

- c. Financial arrangements, including access to data in case of nonpayment or default;
- d. Arrangements upon termination of relationship with SaaS provider, including access to data; and
- e. Nature of confidentiality protections, including password protection and availability of different levels of encryption.

The Opinion further notes that lawyers may be able to discharge their responsibilities by relying on due diligence efforts by non-lawyer personnel with expertise in these areas.

#### Pennsylvania Bar Association Formal Opinion 2011-200

In its recent Formal Opinion 2011-200, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility similarly concluded that attorneys can use cloud computing if stored materials remain confidential, and reasonable steps are taken to protect stored data from risks including security breaches and loss of data. This Pennsylvania Opinion recommends various steps the lawyer should explore with the SaaS vendor, including:

- a. the existence of an obligation imposed on the vendor to preserve security;
- b. a mechanism for the vendor to notify the lawyer if a third party requests access to the stored information;
- c. the existence of systems that are sufficient to protect the data from unauthorized access;
- d. an agreement about how confidential client information will be protected;
- e. the ability to review the vendor's security systems; and
- f. tools to protect the lawyer's ability to access and retrieve the data.

#### California Bar Professional Responsibility and Conduct Committee Formal Op. 2010-179

Recognizing that a technology-specific opinion "would likely become obsolete shortly," California Bar Ethics Opinion 2010-179 similarly endorses Cloud Computing, and then provides a general analysis of the considerations a lawyer should evaluate when using SaaS, including:

- a. The ability of the lawyer to assess the security provided by the provider, including the specifics of the technology, whether specific precautions can be used to increase the level of security, and limits on who is permitted to monitor use of the software, evaluated by someone who possesses a sufficient level of competence to address these issues;
- b. Availability of legal consequences for improper interception of or access to the data;
- c. Degree of sensitivity of the information being stored
- d. Potential impact of unauthorized disclosure on the client;

- e. Urgency of the situation; and
- f. Client circumstances and instructions.

#### New York State Bar Professional Ethics Committee Opinion 842

In September 2010, the New York State Bar Professional Ethics Committee issued a similar opinion, adopting a reasonableness standard and discussing the following factors that a lawyer should consider when storing client information in the cloud:

- a. Confirming that the SaaS vendor has a enforceable duty to maintain security and confidentiality, including prompt notification of the attorney upon service of process requiring disclosure of the data;
- b. Investigating the provider's security procedures, policies, and methods for recovering data;
- c. Guarding against infiltration attempts using available technology;
- d. Determining whether the vendor can transfer and then permanently delete the data if the lawyer changes providers;
- e. Periodically reconfirming that security and access measures remain sufficient as technologies change; and
- f. Remaining current on the law with respect to changing technologies to ensure that client data is not subject to legal risk, including waiver of confidentiality.

#### Other Opinions and Authorities

Ethics opinions issued by other State Bar Associations have taken similar positions.

State Bar of Arizona Ethics Opinion 09-04, for example, reaffirms the conclusion drawn in its prior Ethics Opinion 05-04, and concludes that attorneys can use online storage and retrieval systems for client documents and information as long as they take reasonable precautions to ensure that the materials are safe and confidential. This Arizona Opinion further notes that lawyers should recognize that their expertise with respect to technology may be limited and should therefore ensure review of precautions by competent personnel, and periodically review systems to ensure that security precautions remain reasonable.

Opinion 701 of the New Jersey Advisory Committee on Professional Ethics discusses the benefits that may arise from web-based digital storage of and access to client documents and information, and then provides as follows:

"The critical requirement . . . is that the attorney 'exercise reasonable care' against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access. 'Reasonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can

guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax.”

Opinion 701 continues by noting that the content of the obligation to exercise reasonable care depends on the circumstances and must be informed by the available technology, and personnel handling client information must be subject to an enforceable obligation to preserve confidentiality and security. In addition, Opinion 701 excludes original “client property” from its holding, and notes that lawyers must continue to maintain certain original documents, like wills, trusts, deeds, contracts, and corporate bylaws and minutes, and cannot rely solely on digital storage of these materials. This Opinion further stresses the importance of client consent with respect to remote storage of client information.

To similar effect are Ethics Opinion 2010-02 issued by the Alabama State Bar Association, and Formal Opinion No. 33 issued by the State Bar of Nevada Standing Committee on Ethics and Professional Responsibility. Many other resources also are available about the use of SaaS, including the ABA Commission on Ethics 20/20 Working Group’s September 20, 2010 white papers discussing SaaS, and the Law Society of British Columbia’s July 15, 2011 Report of the Cloud Computing Working Group.

## CONCLUSION

The Vermont Bar Association Professional Responsibility Section agrees with the consensus view that has emerged with respect to use of SaaS. Vermont lawyers’ obligations in this area include providing competent representation, maintaining confidentiality of client information, and protecting client property in their possession. As new technologies emerge, the meaning of “competent representation” may change, and lawyers may be called upon to employ new tools to represent their clients. Given the potential for technology to grow and change rapidly, this Opinion concurs with the views expressed in other States, that establishment of specific conditions precedent to using SaaS would not be prudent. Rather, Vermont lawyers must exercise due diligence when using new technologies, including Cloud Computing. While it is not appropriate to establish a checklist of factors a lawyer must examine, the examples given above are illustrative of factors that may be important in a given situation. Complying with the required level of due diligence will often involve a reasonable understanding of:

- a. the vendor’s security system;
- b. what practical and foreseeable limits, if any, may exist to the lawyer’s ability to ensure access to, protection of, and retrieval of the data;
- c. the material terms of the user agreement;
- d. the vendor’s commitment to protecting confidentiality of the data;
- e. the nature and sensitivity of the stored information;
- f. notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and
- g. other regulatory, compliance, and document retention obligations that may apply based upon the nature of the stored data and the lawyer’s practice.

In addition, the lawyer should consider:

- a. giving notice to the client about the proposed method for storing client data;

- b. having the vendor's security and access systems reviewed by competent technical personnel;
- c. establishing a system for periodic review of the vendor's system to be sure the system remains current with evolving technology and legal requirements; and
- d. taking reasonable measures to stay apprised of current developments regarding

SaaS systems and the benefits and risks they present.

In summary, and with respect to the specific questions posed, the Professional

Responsibility Section responds as follows.

Vermont attorneys may use SaaS systems for storing, processing, and retrieving client property, as long as they take reasonable precautions to ensure the property is secure and accessible. The nature of the precautions depends on the circumstances. The ability to engage in Cloud Computing is not limited by the specific location of the remote server, although some of the factors noted above, including choice of law clauses, and concerns about access to data in the event of a service interruption or an emergency, may be implicated by the location of the storage server and the extent of backup service provided by the vendor.

Depending on the circumstances, there may be limits on systems that can be used and client property that can be stored with an SaaS vendor, and lawyers must assess each situation

based upon the specific facts and circumstances. For example, it may not be appropriate to rely solely on remote digital storage for preservation of original client property like wills, or other client documents that are subject to permanent retention obligations. Similarly, given that Cloud Computing involves storage of information in the hands of a third party, a lawyer handling particularly sensitive client property, like trade secrets may conclude after consultation with the client that remote SaaS storage is not sufficiently secure.

A lawyer's use of email, calendar, and remote synchronization systems, including systems that are web-based and offered by SaaS vendors, is subject to the same inquiry. Before using such systems, the lawyer should take reasonable precautions to ensure that information in the system is secure and accessible.

Finally, given the rapidly changing nature of technology and the significant manner in which new technologies impact the legal practice including the manner in which confidential client information is communicated and stored, the Professional Responsibility Section invites the Vermont Supreme Court to examine whether changes in applicable Rules of Procedure and Rules of Professional Conduct are warranted to address these issues.

**ATTACHMENT S:**  
**Virginia**

This opinion is an examination of the ethical issues involved in a lawyer or firm's use of a virtual law office, including cloud computing, and/or executive office suites. These issues include marketing, supervision of lawyers and nonlawyers in the firm, and competence and confidentiality when using technology to interact with or serve clients.

A virtual law practice involves a lawyer/firm interacting with clients partly or exclusively via secure Internet portals, emails, or other electronic messaging.<sup>1</sup> This practice may be combined with an executive office rental, where a lawyer rents access to a shared office suite or conference room. This space is generally either unstaffed or staffed by an employee of the rental company who provides basic support services to all users of the space, rather than by an employee of the lawyer. The space is also not exclusive to the lawyer – even if she has exclusive access to a particular office or conference room, the suite is open to all other “tenants.” Lawyers who maintain a virtual practice, who work from home, or who wish to expand their geographic profile without the higher costs of exclusive office space and staff all use these spaces as client meeting locations. In other words, virtual law offices and executive office suites do not always go together, but they frequently do.

#### APPLICABLE RULES AND OPINIONS

The applicable Rules of Professional Conduct are Rules 1.1<sup>2</sup>, 1.6(a)<sup>3</sup>, 5.1(a) and (b)<sup>4</sup>, 5.3(a) and (b)<sup>5</sup>, and 7.1<sup>6</sup>. The relevant legal ethics opinions are LEOs 1600, 1791, 1818, and 1850. Finally,

---

<sup>1</sup> Stephanie Kimbro, a practitioner and scholar of virtual law offices, defines a virtual law practice as one where “[t]he use of an online client portal allows for the initiation of the attorney/client relationship through to completion and payment for legal services. Attorneys operate an online backend law office as a completely web-based practice or in conjunction with a traditional law office.” <http://virtuallawpractice.org/about/>, accessed Jan. 22, 2013.

<sup>2</sup> **Rule 1.1      Competence**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

<sup>3</sup> **Rule 1.6      Confidentiality of Information**

(a) A lawyer shall not reveal information protected by the attorney-client privilege under applicable law or other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

(b) To the extent a lawyer reasonably believes necessary, the lawyer may reveal:

\*\*\*

(6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

<sup>4</sup> **Rule 5.1      Responsibilities of Partners and Supervisory Lawyers**

(a) A partner in a law firm, or a lawyer who individually or together with other lawyers possesses managerial authority, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

Regulation 7 Governing Applications for Admission to the Virginia Bar Pursuant to Rule 1A:1 of the Supreme Court of Virginia applies to lawyers who are admitted or seeking admission by motion to the Bar of Virginia<sup>7</sup>.

## ANALYSIS

Virtual law offices involve issues that are present in all types of law offices – confidentiality, communication with clients, and supervision of employees – but that manifest themselves in a new way in this context. *See also* LEO 1850 (exploring similar concerns in context of outsourcing legal support services).

A lawyer must always act competently to protect the confidentiality of clients' information, regardless of how that information is stored/transmitted, but this task may be more difficult when the information is being transmitted and/or stored electronically through third-party software and storage providers. The lawyer is not required, of course, to absolutely guarantee that a breach of confidentiality cannot occur when using an outside service provider. Rule 1.6 only requires the lawyer to act with reasonable care to protect information relating to the representation of a client. When a lawyer is using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data, the lawyer must

---

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

### <sup>5</sup> **Rule 5.3 Responsibilities Regarding Nonlawyer Assistants**

With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (a) a partner or a lawyer who individually or together with other lawyers possesses managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
- (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and...

### <sup>6</sup> **Rule 7.1 Communications Concerning a Lawyer's Services**

(a) A lawyer shall not, on behalf of the lawyer or any other lawyer affiliated with the lawyer or the firm, use or participate in the use of any form of public communication if such communication contains a false, fraudulent, misleading, or deceptive statement or claim.

\*\*\*

<sup>7</sup> **7. Intent to Practice Full Time in Virginia.** An applicant must intend, promptly after being admitted to practice in Virginia without examination, to establish his or her office in Virginia and to practice full time from such Virginia office. Full time is defined as being engaged in the active practice of law (as defined above) as one's primary occupation for at least thirty-five (35) hours weekly and having an office where clients can be seen on the premises. The Board shall not approve an application unless the applicant has verifiable plans to practice in Virginia (*i.e.*, a job offer from a Virginia firm, a relocation to the Virginia office of the applicant's firm, an executed lease for office space in Virginia, etc.). Practice from one's residence shall not constitute satisfactory evidence of intent to practice law full time unless the applicant's residence is in a zoning classification which permits seeing clients on the premises and displaying an exterior sign identifying the law office. Virtual offices or shared occupancy arrangements shall not be acceptable. In addition, an applicant shall not divide his or her time between an office within Virginia and one in another jurisdiction. An applicant who is a member of or associated with a firm which has offices outside Virginia must be resident at such firm's Virginia office, shall not maintain an office at a location outside Virginia, and may work at one of his or her firm's other offices only on an occasional and not on a regular basis. The Court will monitor to determine whether an applicant maintains his or her Virginia office.

follow Rule 1.6(b)(6) and exercise care in the selection of the vendor, have a reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and instruct the vendor to preserve the confidentiality of the information. The lawyer will have to examine the third party provider's use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination.<sup>8</sup>

Similarly, although the method of communication does not affect the lawyer's duty to communicate with the client, if the communication will be conducted primarily or entirely electronically, the lawyer may need to take extra precautions to ensure that communication is adequate and that it is received and understood by the client. The Committee previously concluded in LEO 1791 that a lawyer could permissibly represent clients with whom he had no in-person contact, because Rule 1.4 "in no way dictates whether the lawyer should provide that information in a meeting, in writing, in a phone call, or in any particular form of communication. In determining whether a particular attorney has met this obligation with respect to a particular client, what is critical is *what* information was transmitted, not *how*." On the other hand, one of the aspects of communication required by Rule 1.4 is that a lawyer must "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Use of the word "explain" necessarily implies that the lawyer must take some steps beyond merely providing information to make sure that the client actually is in a position to make informed decisions. A lawyer may not simply upload information to an Internet portal and assume that her duty of communication is fulfilled without some confirmation from the client that he has received and understands the information provided.

Finally, the technology that enables a lawyer to practice "virtually" without any face-to-face contact with clients can also allow lawyers and their staff to work in separate locations rather than together in centralized offices. As with other issues discussed in this opinion, a partner or other managing lawyer in a firm always has the same responsibility to take reasonable steps to supervise subordinate lawyers and nonlawyer assistants, but the meaning of "reasonable" steps may vary depending upon the structure of the law firm and its practice. Additional measures may be necessary to supervise staff who are not physically present where the lawyer works.

The use of an executive office/suite rental or any other kind of shared, non-exclusive space, either in conjunction with a virtual law practice or as an addition to a "traditional" office-based practice, raises a separate issue. A non-exclusive office space or virtual law office that is advertised as a location of the firm must be an office where the lawyer provides legal services. Depending on the facts and circumstances, it may be improper under Rule 7.1 for a lawyer to list or hold out a rented office space as her "law office" on letterhead or other public communications. Factors to be considered in making this determination include the frequency with which the lawyer uses the space, whether nonlawyers also use the space, and whether

---

<sup>8</sup> See LEO 1818, where the Committee concluded that a lawyer could permissibly store files electronically and destroy all paper documents as long as the client was not prejudiced by this practice, but noted that the lawyer may need to consult outside technical assistance and support for assistance in using such a system.

signage indicates that the space is used as a law office. In addition, a lawyer may not list alternative or rented office spaces in public communications for the purpose of misleading prospective clients into believing that the lawyer has a more geographically diverse practice and/or more firm resources than is actually the case. As discussed above in the context of Internet-based service providers, a lawyer must also pay careful attention to protecting confidentiality if any client information is stored or received in a shared space staffed by nonlawyers who are not employees of the law firm and may not be aware of the nature or extent of the duty of confidentiality.

For lawyers who are licensed to practice in Virginia by motion rather than by bar exam, Regulation 7 of the Regulations Governing Applications for Admission to the Virginia Bar Pursuant to Rule 1A:1 of the Supreme Court of Virginia creates an additional difficulty in using an executive office rental or virtual office. This Regulation requires that a lawyer who is seeking admission, or who is already admitted, by motion maintain an office in Virginia where clients can be seen on the premises, and specifically provides that virtual office or shared occupancy arrangements are not acceptable for purposes of satisfying the office requirement.<sup>9</sup> Accordingly, a lawyer who is admitted by motion should first ensure that any office space arrangement complies with Regulation 7 before there is any need to consider the ethics issues raised.

This opinion is advisory only and is not binding on any court or tribunal.

Committee Opinion

March 29, 2013

---

<sup>9</sup> *But see* Proposed Amendments to Rules 1A:1 and 1A:3, proposed October 22, 2012, available at [http://courts.state.va.us/news/draft\\_revisions\\_rules/2012\\_rules\\_1\\_3\\_draft.pdf](http://courts.state.va.us/news/draft_revisions_rules/2012_rules_1_3_draft.pdf) (proposing change to requirements for admission by waiver from “full-time” practice requirement to “predominant” practice requirement).

**ATTACHMENT T:  
Washington**



**Advisory Opinion:** 2215

**Year Issued:** 2012

**RPC(s):** RPC 1.1, 1.6, 1.15A

**Subject:** Cloud Computing

---

This opinion addresses certain ethical obligations related to the use of online data storage managed by third party vendors to store confidential client documents.

**Illustrative Facts:**

Law Firm contracts with third-party vendor to store client files and documents online on remote server so that Lawyer and Client could access the documents over the Internet from any remote location.

**Rules of Professional Conduct Implicated:**

RPC 1.1, 1.6, 1.15A

**Analysis:**

Various service providers are offering data storage systems on remote servers that can be accessed by subscribers from any location over the Internet. This is one aspect of so-called “cloud computing,” and lawyers may be interested in using these services to store confidential client documents and other data. Use of these third party storage systems, however, means that confidential client information is outside of the direct control of the lawyer and raises particular ethical questions.

Under RPC 1.6, a lawyer owes a client the duty to keep all client information confidential, unless the information falls within a specified exception. The duty of confidentiality extends beyond deliberate revelations of client information and requires a lawyer to protect client information against all disclosure. Comment 16 to RPC 1.6 states: “A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3.” In order to use online data storage, a lawyer is under a duty to ensure that the confidentiality of all client data will be maintained.

In addition to client confidentiality, the lawyer is also under a duty to protect client property, under RPC 1.15A. A lawyer using online data storage of client documents is therefore under a duty to ensure that the documents will not be lost.

It is impossible to give specific guidelines as to what security measures should be in place with a third party service provider of online data storage in order to provide adequate protection of client material, because the technology is changing too rapidly and any such advice would be quickly out of date. It is also impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's security systems. A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so. While some lawyers may be able to do more thorough evaluations of the services available, best practices for a lawyer without advanced technological knowledge could include:

1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
2. Evaluation of the provider's practices, reputation and history.
3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer's stored data.
6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.
7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider.

A lawyer has a general duty of competence under RPC 1.1, which includes the duty "to keep abreast of changes in the law and its practice." RPC 1.1 Comment 6. To the extent that a lawyer uses technology in his or her practice, the lawyer has a duty to keep informed about the risks associated with that technology and to take reasonable precautions. The lawyer's duties discussed in this opinion do not rise to the level of a guarantee by the lawyer that the information is secure from all unauthorized access. Security breaches are possible even in the physical world, and a lawyer has always been under a duty to make reasonable

judgments when protecting client property and information. Specific practices regarding protection of client property and information have always been left up to individual lawyers' judgment, and that same approach applies to the use of online data storage. The lawyer must take reasonable steps, however, to evaluate the risks involved with that practice and to ensure that steps taken to protect the information are up to a reasonable standard of care.

Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider. Over time, a particular provider's security may become obsolete or become substandard to systems developed by other providers.

## Conclusion

A lawyer may use online data storage systems to store and back up client confidential information as long as the lawyer takes reasonable care to ensure that the information will remain confidential and that the information is secure against risk of loss.

Advisory Opinions are provided for the education of the Bar and reflect the opinion of the Rules of Professional Conduct Committee. Advisory Opinions are provided pursuant to the authorization granted by the Board of Governors, but are not individually approved by the Board and do not reflect the official position of the Bar association. Laws other than the Washington State Rules of Professional Conduct may apply to the inquiry. The Committee's answer does not include or opine about any other applicable law than the meaning of the Rules of Professional Conduct. Advisory Opinions are based upon facts of the inquiry as presented to the committee.