§ 3-501.1. Competence.

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

COMMENT

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal

problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] In an emergency, a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a 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. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(b).

Maintaining Competence

[6] 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

§ 3-501.1 Comment 6 amended June 28, 2017.

‹ §§ 3-501.1 to 3-501.18: Client-Lawyer Relationship | up | § 3-501.2. Scope of representation and allocation of authority between client and lawyer. ›

§ 3-501.6. 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 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 prevent the client from committing a crime or to prevent reasonably certain death or substantial bodily harm;

(2) to secure legal advice about the lawyer's compliance with these Rules;

(3) to establish a claim or defense on behalf of the lawyer in a 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; or

(4) to comply with other law or a court order.

(c) The relationship between a member of the Nebraska State Bar Association Committee on the Nebraska Lawyers Assistance Program or an employee of the Nebraska Lawyers Assistance Program and a lawyer who seeks or receives assistance through that committee or that program shall be the same as that of lawyer and client for the purposes of the application of Rule 1.6.

COMMENT

[1] This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

[2] 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. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work-product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope .

[4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. A lawyer may disclose information relating to the representation necessary to prevent a client from committing a crime. Paragraph (b)(1) also recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. For example, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims.

[7] A lawyer’s confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer’s personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(2) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

[8] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, for example, a person claiming to have been defrauded by the lawyer and client acting together. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(3) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

[9] A lawyer entitled to a fee is permitted by paragraph (b)(3) to prove the services rendered in an action to collect This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[10] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(4) permits the lawyer to make such disclosures as are necessary to comply with the law.

[11] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4 . Unless review is sought, however, paragraph (b)(4) permits the lawyer to comply with the court's order.

[12] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[13] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(4) . In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the nature of the future crime, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b) . See Rules 1.2(f), 4.1(b) , 8.1 and 8.3 . Rule 3.3 , on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c) .

Withdrawal

[14] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw, as stated in Rule 1.16(a)(1) . After withdrawal, the lawyer is required to refrain from making disclosure of the client's confidences, except as otherwise permitted by Rule 1.6. Neither this Rule nor Rule 1.8(b) nor Rule 1.16(d) prevents the lawyer from giving notice of the fact of withdrawal, and the lawyer may also withdraw or disaffirm any opinion, document, affirmation, or the like. Where the client is an organization, the lawyer may be in doubt whether contemplated conduct will actually be carried out by the organization. Where necessary to guide conduct in connection with this Rule, the lawyer may make inquiry within the organization as indicated in Rule 1.13(b).

Acting Competently to Preserve Confidentiality

[15] 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 .

[16] 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.

Former Client

[17] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2) . See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

Comment [13] amended September 7, 2016.

Nebraska Ethics Advisory Opinion for Lawyers
No. 17-01

QUESTION PRESENTED

When a client file is closed, is it permissible to make an electronic copy of the file and then destroy the physical file immediately?

Brief Answer

The Nebraska Rules of Professional Conduct do not prohibit an attorney from keeping a closed client file in electronic form and immediately destroying the physical copy. However, several factors should be considered before a file is destroyed, such as whether it would be in the best interest of the client to keep the physical/paper copy and whether physical/paper copies of documents will be needed to satisfy the original document rule.

FACTS

A legal services organization has asked about file retention requirements under the Nebraska Rules of Professional Conduct. The organization currently retains the physical/paper copy of its clients' files for seven years. Physical storage space has become an issue, so it is considering the use of current technology that involves scanning its closed files and digitally storing the scanned images in lieu of physical storage.

Applicable Rules of Professional Conduct

Section 3-501.15(a): "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. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated. 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 a period of 5 years after termination of the representation."

Section 3-501.16(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 or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law."

Discussion

There are no specific rules of professional conduct that address the requirements of lawyers to retain a physical copy of a file instead of an electronic copy. However, some factors should be considered before destroying the physical file and retaining only a digital file. As stated in Opinion 88-3, "the retention or destruction of client files is primarily a matter of good judgment. . ." That decision is no longer controlling, pursuant to Opinion 12-07, but much of the logic and reason of the opinion still offer sound guidance. Since its drafting, the adoption of the Model Rules of Professional Conduct stated a minimum time which files must be retained. The rule now states that other property shall be preserved for a period of five (5) years. Opinion 12-07 listed several factors to consider with regard to the retention of files:

1. The file may include original documents or other property furnished by or on behalf of the client, the return of which might reasonably be expected by the client. Before destroying such documents or property, the client should be asked whether he wants delivery of them. Alternatively, the lawyer may simply deliver such documents to the client with appropriate advice regarding factors which the client should consider in determining which items to preserve. Where unable to contact the client, the lawyer should be guided by the foreseeable need for the documents in determining whether to destroy them.

2. An attorney must use care not to destroy or discard information that he knows or should know may still be necessary or useful in the assertion or defense of the client's position in a matter for which a statute of limitations has not expired.

3. An attorney must consider the reasonable expectations of the client for the preservation of files.

4. The nature and contents of some files may indicate a need for longer retention than do the nature and contents of other files, based upon their relevance and materiality to matters that can be expected to arise in the future.

5. Disposition of client files must be made in such a manner as to protect full the confidentiality of the contents.

The State Bar of Arizona discussed the digital retention of client files in some detail. Arizona Informal Opinion 07-02 (2007) emphasized that a lawyer must make considerations such as the ability of the client to be able to open and access the electronic file format, assuring that the digitized file is complete and accurate, receiving consent from the client to digitize the file, and returning the hard copy to the client after digitizing it. The Arizona committee found that in appropriate cases, with careful consideration of the effects on a client, a lawyer may digitally store client files.

In considering the obligation of an attorney to provide a file to a client, this committee stated in Opinion 12-09 that production of a file to the client may be accomplished by a scanned or hard copy. This necessarily means that retaining a scanned copy of a client file should comply with the Rules of Professional Conduct. However, there might be unique circumstances where maintaining a paper copy of a client file would outweigh the convenience of an electronically stored copy (e.g. large items such as architectural/engineering plans, large photos, items that might be costly to reproduce from digital to paper). The same considerations should be applied when determining whether the physical file should be destroyed with only a digital copy being retained. The reasonable expectations of the client must be considered.

Other considerations may include, but are not limited to, the potential need for a physical copy at trial, the original document rule, or the client's or lawyer's future use of the physical file. The original document rule states, "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Neb. Rev. Stat. § 27-1003 (Reissue 2008). Thus, an attorney should consider if an original document will be needed to satisfy the original document rule in future litigation. In addition, it was stated in opinion 12-07 that an attorney should make reasonable efforts to contact the client regarding the importance of the documents in the physical file after the file is closed.

Conclusion

Given the impact of technology on how files can be retained, it is not reasonable or practical keep physical/paper copies of every client file. Factors to consider include: availability and cost of physical and electronic storage space, ease of access to documents, potential need for originals in future litigation, and preserving confidentiality. It is reasonable for an organization to digitize its closed files. However, the organization must consider the factors noted above and any other considerations that are pertinent to the contents of a particular file. A written procedure for file retention and ultimate destruction of physical and digital copies of the contents of files should be maintained, followed, and revised as needed.

Nebraska Ethics Advisory Opinion for Lawyers
No. 06-5

ETHICAL ISSUES

I. WHETHER THERE ARE ANY ETHICAL ISSUES INVOLVED IN SHARING A COMPUTER SERVER WITH VARIOUS COUNTY OFFICES.

II. WHETHER A PUBLIC DEFENDER IS REQUIRED TO USE ITS OWN COMPUTER SERVER.

STATEMENT OF FACTS

A public defender's office shares a computer server with other county offices, such as the county sheriff's office and the county attorney, among others. The public defender maintains a database for clients which database is stored in a program within the server. The database contains information regarding the names of clients, addresses, and some case information. The county employs an IT director and various employees who have access to the client database maintained by the public defender.

NEBRASKA RULES OF PROFESSIONAL CONDUCT

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, 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 prevent the client from committing a crime or to prevent reasonably certain death or substantial bodily harm;
(2) to secure legal advice about the lawyer's compliance with these Rules;
(3) to establish a claim or defense on behalf of the lawyer in a 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; or
(4) to comply with other law or a court order.

OTHER SOURCES

There are no Nebraska Advisory Opinions that the Committee could locate which were directly on point. However, the Advisory Committee believes that the present situation can be analogized to opinions in which ethical considerations were considered in "office sharing" arrangements. The Advisory Committee has dealt with office sharing arrangements in past opinions. Though the opinions were issued based on the Nebraska Code of Professional Responsibility instead of the recently enacted Nebraska Rules of Professional Conduct, and involved true office sharing arrangements, they are still useful in evaluating the present situation.

The past opinions have addressed the issue of individual attorneys sharing office space and resources, such as staff, conference rooms, reception areas, copiers, telephones, and computer systems. Past opinions have noted the potential ethical issues of confidentiality, conflicts of interest, and the appearance of impropriety in such situations. It is apparent that on occasion the imputation of conflicts can occur even when attorneys have no intention of being associated with each other, but merely share resources and are not officially affiliated with each other. It is not known whether the county attorney's office has access to the public defender's client files saved on the server, but this opinion includes a brief discussion of conflicts of interest and imputation of

conflicts in the event the county attorney does have access to those same client files which are stored on a common server.

DISCUSSION

This discussion should be prefaced with the consideration that criminal defendants are guaranteed the right to counsel under the Sixth Amendment of the United States Constitution. See Montana Ethics Opinion 960924 (1996). This right to counsel for criminal defendants includes the right to be represented by an attorney who is free of any possible conflicts of interest. Id. (citing Wood v. Georgia, 450 U.S. 261, 271 (1981)). While a high level of vigilance is required in the representation of any client, there are these additional constitutional issues to consider in the representation of criminal clients.

The first issue is that of the potential for confidential information from criminal files being viewed by individuals outside the public defender's office. In one 1989 Nebraska Advisory Opinion, individual attorneys maintained private offices, but shared a receptionist, secretaries, a library, a computer system, and conference rooms. The computer system was designed, to the extent possible, to ensure that each attorney would have access only to his own material. As the Advisory Committee noted at the time, the issue was whether the sharing of various resources constituted a sharing of offices by the attorneys, thus precluding one attorney from accepting a case which the other cannot ethically accept. While this opinion is not entirely on point with the instant situation, it is instructive. The opinion specifically sets forth requirements for a situation in which two separate attorneys share office space and resources, without invoking the possibility for conflicts. The opinion states that the attorneys may represent adverse parties so long as the following precautions were met:

(1) There shall be no common access to any case files;
(2) There shall be no common access to any computerized data relating to the case;
(3) No secretary shall be allowed to work on the case for both parties;
(4) All common employees shall be informed of the adverse representation and the extreme sensitivity to the maintenance of confidentiality; and
(5) Each client shall give his consent to the adverse representation after full disclosure of all facts relating to the common practice areas.

Formal Opinion 89-2 (March 31, 1989). The Advisory Committee based these precautions upon DR 4-101(D) under the Nebraska Code of Professional Responsibility, which provided that a lawyer shall exercise reasonable care to prevent the disclosure of confidences or secrets of the clients.

A 2002 Advisory Opinion addressed this same issue, with the Committee noting that the precautions set forth in Formal Opinion 89-2 were still valid. The Committee concluded that while there was no conflict of interest under the facts of that situation, any sharing of computer files or paper files puts client confidences at risk. The Committee cited to an article in the ABA/BNA Lawyer's Manual on Professional Conduct, emphasizing the necessity of physically organizing an office so as to avoid putting client confidences at risk. Specifically:

Access to Files: The office-sharing lawyers cannot have access to each other's files.

Computers: The lawyers must avoid sharing computers and any sensitive information often located in the computer system.

Formal Opinion 02-2 (citing the ABA/BNA Lawyer's Manual on Professional Conduct 91:605). The Advisory Committee also clarified its position on shared file and computer systems. It stated that:

1. The attorney shall keep a secure file system, only accessible to the attorney and the attorney's staff.
2. The attorney shall keep a secure computer system, only accessible to the attorney and the attorney's staff.

Formal Opinion 02-2.

Other states have recognized similar principles in maintaining client confidentiality in situations in which attorneys do not maintain sole access to their computer systems. In a Colorado opinion, the Colorado Ethics Committee noted that:

[o]ffice sharing lawyers should be particularly attentive when lawyers or their employees have access to each other's file storage and/or have shared…computer and telephone equipment…. The more shared equipment…the greater potential for inadvertent disclosure of client confidences and secrets and…such disclosure will be harmful to the client.

Colorado Ethics Opinion 89 (Adopted September 21, 1991; amended April 18, 1992). The opinion further states:

[t]o ensure confidentiality, the office sharing lawyer may need to take certain measures in addition to restricting access to files, such as restricting access between the telephone systems of the separate practices[,]… using security devices to restrict access to computers[,]… and informing clients of the space sharing arrangement and of measures undertaken to avoid any compromise of confidentiality.

Id. (citing Indiana Ethics Opinion 8 of 1985 (undated)).

The issue of potential conflicts in similar situations is far from being uniformly settled from state to state. While all of the various state ethics opinions have recognized that there are potential confidentiality issues, the state opinions have ranged from "flatly prohibitive" to "generally permissive." Nebraska Advisory Opinion 89-2. In Formal Opinion 89-2, this Committee noted that discussions generally referred to two Canons under the Code of Professional Responsibility, Canon 4, the preservation of confidences and secrets of clients, and Canon 9, the avoidance of the appearance of professional impropriety. Canon 4 is now codified in newly adopted Rule 1.6 relating to the confidentiality of client information.

CONCLUSION

The Nebraska Advisory Committee offers the following guidance in response to the stated ethical concerns:

The employees of the public defender's office must be the only individuals who have access to client information, including that which is stored on the computer system. If any component of the computer system is linked or somehow shared by other county offices, the public defender must take whatever reasonable and necessary precautions there are to ensure that this information cannot be accessed by the other offices. This is the public defender's primary responsibility in this scenario. If the public defender is not satisfied that client confidentiality can be secured, then the ethical alternative is to either maintain a separate computer system from the other county offices or discontinue storing client information on the shared system.

Nebraska Ethics Advisory Opinion for Lawyers
No. 06-5

Nebraska Ethics Advisory Opinion for Lawyers
No. 02-2

DOES THE CODE OF PROFESSIONAL RESPONSIBILITY PERMIT AN ATTORNEY WHO SHARES OFFICE SPACE WITH A PUBLIC DEFENDER TO ACCEPT APPOINTMENTS AS DEFENSE COUNSEL IN CRIMINAL MATTERS WHERE THE PRESENT PUBLIC DEFENDER HAS A CONFLICT OF INTEREST? IN RESPONSE TO THE REQUEST FOR AN OPINION FROM THIS COMMITTEE, WE FURNISH THE FOLLOWING.

RESTATEMENT OF FACTS

You share office space with the newly elected County Public Defender. Your practices are generally operated independently in that each of you has his own staff, phone lines and computer system, although there is some expense sharing. In the past, you have been appointed as defense counsel in criminal matters where the present Public Defender has a conflict of interest. You would prefer to continue to accept these appointments after the newly elected Public Defender takes office.

STATEMENT OF APPLICABLE CANONS AND DISCIPLINARY RULES

EC 1-1. A basic tenet of the professional responsibility of lawyers is that every person in our society should have ready access to the independent professional services of a lawyer of integrity and competence. Maintaining the integrity and improving the competence of the bar to meet the highest standards is the ethical responsibility of every lawyer.

Canon 2: A lawyer should assist the legal profession in fulfilling its duty to make legal counsel available.

EC 2-25. Historically, the need for legal services of those unable to pay reasonable fees has been met in part by lawyers who donated their services or accepted court appointments on behalf of such individuals. The basic responsibility for providing legal services for those unable to pay ultimately rests upon the individual lawyer, and personal involvement in the problems of the disadvantaged can be one of the most rewarding experiences in the life of a lawyer. Every lawyer, regardless of professional prominence or professional workload, should find time to participate in serving the disadvantaged. The rendition of free legal services to those unable to pay reasonable fees continues to be an obligation of each lawyer, but the efforts of individual lawyers are often not enough to meet the need. Thus it has been necessary for the profession to institute additional programs to provide legal services. Accordingly, legal aid offices, lawyer referral services, and other related programs have been developed, and others will be developed, by the profession. Every lawyer should support all proper efforts to meet this need for legal services.

EC 2-26. A lawyer is under no obligation to act as adviser or advocate for every person who may wish to become the lawyer's client; but in furtherance of the objective of the bar to make legal services fully available, a lawyer should not lightly decline proffered employment. The fulfillment of this objective requires acceptance by a lawyer of his or her share of tendered employment which may be unattractive both to him or her and the bar generally.

EC 2-29. When a lawyer is appointed by a court or requested by a bar association to undertake representation of a person unable to obtain counsel, whether for financial or other reasons, he or she should not seek to be excused from undertaking the representation except for compelling reasons. Compelling reasons do not include such factors as the repugnance of the subject matter of the proceeding, the identity or position of a person involved in the case, the belief of the lawyer that the defendant in a criminal proceeding is guilty, or the belief of the lawyer regarding the merits of the civil case.

Canon 4: A lawyer should preserve the confidences and secrets of a client.

EC 4-1. Both the fiduciary relationship existing between lawyer and client and the proper functioning of the legal system require the preservation by the lawyer of confidences and secrets of one who has

employed or sought to employ him or her. A client must feel free to discuss whatever the client wishes with his or her lawyer and a lawyer must be equally free to obtain information beyond that volunteered by the client. A lawyer should be fully informed of all the facts of the matter the lawyer is handling in order for his or her client to obtain the full advantage of our legal system. It is for the lawyer in the exercise of the lawyer's independent professional judgment to separate the relevant and important from the irrelevant and unimportant. The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of a client not only facilitates the full development of facts essential to proper representation of the client but also encourages laypersons to seek early legal assistance.

EC 4-4. The lawyer-client privilege is more limited than the ethical obligation of a lawyer to guard the confidences and secrets of his or her client. This ethical precept, unlike the evidentiary privilege, exists without regard to the nature or source of information or the fact that others share the knowledge. A lawyer should endeavor to act in a manner which preserves the evidentiary privilege; for example, the lawyer should avoid professional discussions in the presence of persons to whom the privilege does not extend. A lawyer owes an obligation to advise the client of the lawyer-client privilege and timely to assert the privilege unless it is waived by the client.

EC 4-5. A lawyer should not use information acquired in the course of the representation of a client to the disadvantage of the client and a lawyer should not use, except with the consent of the lawyer's client after full disclosure, such information for his or her own purposes. Likewise, a lawyer should be diligent in his or her efforts to prevent the misuse of such information by the lawyer's employees and associates. Care should be exercised by a lawyer to prevent the disclosure of the confidences and secrets of one client to another and no employment should be accepted that might require such disclosure.

Canon 5: A lawyer should exercise independent professional judgment on behalf of a client.

EC 5-1. The professional judgment of a lawyer should be exercised, within the bounds of the law, solely for the benefit of the lawyer's client and free of compromising influences and loyalties. Neither the lawyer's personal interests, the interests of other clients, nor the desires of third persons should be permitted to dilute the lawyer's loyalty to his or her client.

EC 5-15. If a lawyer is requested to undertake or to continue representation of multiple clients having potentially differing interests, the lawyer must weigh carefully the possibility that his or her judgment may be impaired or his or her loyalty divided if he or she accepts or continues the employment. The lawyer should resolve all doubts against the propriety of the representation. A lawyer should never represent in litigation multiple clients with differing interests; and there are few situations in which a lawyer would be justified in representing in litigation multiple clients with potentially differing interests. If a lawyer accepted such employment and the interests did become actually differing, he or she would have to withdraw from employment with likelihood of resulting hardship on the clients; for this reason, it is preferable that the lawyer refuse the employment initially. On the other hand, there are many instances in which a lawyer may properly serve multiple clients having potentially differing interests in matters not involving litigation. If the interests vary only slightly, it is generally likely that the lawyer will not be subjected to an adverse influence and that the lawyer can retain his or her independent judgment on behalf of each client; if the interests become differing, withdrawal is less likely to have a disruptive effect upon the causes of his or her clients.

EC 5-16. In those instances in which a lawyer is justified in representing two or more clients having differing interests, it is nevertheless essential that each client be given the opportunity to evaluate his or her need for representation free of any potential conflict and to obtain other counsel if he or she so desires. Thus before a lawyer may represent multiple clients, the lawyer should explain fully to each client the implications of the common representation and should accept or continue employment only if the clients consent. If there are present other circumstances that might cause any of the multiple clients to question the undivided loyalty of the lawyer, he or she should also advise all of the clients of those circumstances.

EC 5-17. Typically recurring situations involving potentially differing interests are those in which a lawyer is asked to represent codefendants in a criminal case, co-plaintiffs in a personal injury case, an insured and

his or her insurer, and beneficiaries of the estate of a decedent. Whether a lawyer can fairly and adequately protect the interests of multiple clients in these and similar situations depends upon an analysis of each case. In certain circumstances, there may exist little chance of the judgment of the lawyer being adversely affected by the slight possibility that the interests will become actually differing; in other circumstances, the chance of adverse affect upon the lawyer's judgment is not unlikely.

Canon 9: A lawyer should avoid even the appearance of professional impropriety.

DISCUSSION

The general concept of conflicts of interest in an office sharing arrangement has previously been addressed by this Committee in Formal Opinion 89-2 (modifying prior Formal Opinion 75-13). There, the following conclusion was reached:

Lawyers who maintain separate and independent practices but share certain office facilities, including reception area, conference rooms, library, computer systems, and receptionist and secretarial personnel, may represent adverse parties so long as the following precautions are met:

1. There shall be no common access to the case files;
2. There shall be no common access to any computerized data relating to the case;

3. No secretary shall be allowed to work on the case for both parties;

4. All common employees shall be informed of the adverse representation and the extreme sensitivity to the maintenance of confidentiality; and

5. Each client shall give his/her consent to the adverse representation after full disclosure of all facts relating to the common practice area.

This topic was addressed more recently by the Nebraska Supreme Court in State v. Fletcher, 253 Neb. 1029; 573 N.W.2d 752 (1998). In that case, defense counsel rented space from a member of the public defender's firm (who represented a codefendant). The defense counsel testified in the hearing for post-conviction relief that he was an independent practitioner and that he did not recall sharing any information with the Public Defender which could not have been found in police reports or in other sources. Further, the defendant did not introduce any evidence to support his claim that he was prejudiced by the agreement between the attorneys, and testified that he could not prove any confidential communications he had with his attorney were made known to the Public Defender. The Court ruled:

Although we conclude there is not a conflict in this case, we point out that both the trial court and the practicing bar should be cognizant of the mischief that can be created in the appointment of defense counsel who has an office-sharing arrangement with counsel for a codefendant.

It would seem from this case and our prior opinion that it would be inappropriate for this Committee to determine that there is an automatic conflict where attorneys share office space. However, it would seem appropriate to review the precautions that should be applied to this situation.

This view seems to be consistent with the views of many states as discussed in an article beginning at page 91:605 of the ABA/BNA Lawyer's Manual on Professional Conduct. That article emphasizes the necessity of physically organizing the office in a way that puts client confidences at risk. The specific items discussed are:

Access to Files: The office-sharing lawyers cannot have access to each other's files.

Personnel: Although a common receptionist is permissible, the lawyers should not share secretaries or other support personnel who have access to sensitive or privileged materials.

Computers: The lawyers must avoid sharing computers and any sensitive information often located in the computer system.

Fax Machines: At the very least, access to fax machines should be restricted or it should be made clear to potential users that fax communications are not private.

Copy Machines: The lawyers must either restrict access to copiers or take care not to leave sensitive materials in the machine.

Telephones: Although the office-sharers may share a receptionist, they must ensure that the employees of one lawyer cannot access telephone conversations of the other.

Formal Opinion 89-2 addresses the first three of the above concerns, but we now clarify the first two of those concerns by restating them as follows:

1. The attorney shall keep a secure file system, only accessible to the attorney and the attorney's staff.

2. The attorney shall keep a secure computer system, only accessible to the attorney and the attorney's staff.

In order to cover the last three items, we add the following additional precaution:

The attorney shall insure that faxes are only available to the attorney and the attorney's staff or it should be made clear to clients where conflicts exist that fax communications to a shared fax machine are not private. In addition, sensitive materials shall not be left in shared copy machines, and the phone system shall be set up so that employees of one lawyer cannot access or listen in on telephone conversations of the other.

With respect to the specific concerns raised in your request for an opinion, it is recommended that all files for cases where conflicts exist be kept in a locked cabinet or office where there is limited chance for access, either accidentally or intentionally. With respect to the consent concern, it is suggested that either consent be obtained immediately following the appointment, or perhaps the judges involved could be requested to explain the conflict at the time of the appointment.

CONCLUSION

It is our opinion that lawyers who maintain separate and independent practices but share office facilities, including an attorney who shares office space with a Public Defender, may represent adverse parties so long as the following precautions are met:

1. The attorney shall keep a secure file system, only accessible to the attorney and the attorney's staff.

2. The attorney shall keep a secure computer system, only accessible to the attorney and the attorney's staff

3. No secretary shall be allowed to work on the case for both parties;

4. All common employees shall be informed of the adverse representation and the extreme sensitivity to the maintenance of confidentiality;

5. Each client shall give his/her consent to the adverse representation after full disclosure of all facts relating to the common practice area; and

6. The attorney shall insure that faxes are only available to the attorney and the attorney's staff or it

should be made clear to clients where conflicts exist that fax communications to a shared fax machine are not private. In addition, sensitive materials shall not be left in shared copy machines, and the phone system shall be set up so that employees of one lawyer cannot access or listen in on telephone conversations of the other.

December 18, 2002

Nebraska Ethics Advisory Opinion for Lawyers
No. 02-2

Nebraska Ethics Advisory Opinion for Lawyers
No. 89-2

Opinion No. 75-13 Modified.

LAWYERS WHO MAINTAIN SEPARATE AND INDEPENDENT PRACTICES BUT SHARE CERTAIN OFFICE FACILITIES, INCLUDING RECEPTION AREA, CONFERENCE ROOMS, LIBRARY, COMPUTER SYSTEMS, AND RECEPTIONIST AND SECRETARIAL PERSONNEL, MAY REPRESENT ADVERSE PARTIES SO LONG AS THE FOLLOWING PRECAUTIONS ARE MET:

1. THERE SHALL BE NO COMMON ACCESS TO THE CASE FILES;

2. THERE SHALL BE NO COMMON ACCESS TO ANY COMPUTERIZED DATA RELATING TO THE CASE;

3. NO SECRETARY SHALL BE ALLOWED TO WORK ON THE CASE FOR BOTH PARTIES;

4. ALL COMMON EMPLOYEES SHALL BE INFORMED OF THE ADVERSE REPRESENTATION AND THE EXTREME SENSITIVITY TO THE MAINTENANCE OF CONFIDENTIALITY; AND

5. EACH CLIENT SHALL GIVE HIS/HER CONSENT TO THE ADVERSE REPRESENTATION AFTER FULL DISCLOSURE OF ALL FACTS RELATING TO THE COMMON PRACTICE AREA.

FACTS

An attorney proposes to develop an area where individual attorneys may have private offices and at the same time share certain costs. The proposal provides that the receptionist, secretaries, library, computer system, and conference rooms would be shared by the attorneys. Each attorney would have his/her own stationery, professional card and telephone line. The computer system would be designed, as nearly as possible, to insure that each attorney would have access

only to his/her own material. There would be no indication of affiliation among the lawyers occupying the premises other than the fact of physical proximity and sharing of certain personnel and facilities.

QUESTION PRESENTED

Under the circumstances as stated above, may an attorney in the office represent a client with interests adverse to those of a client represented by another attorney in the same office?

DISCUSSION

Opinion 75-13 states that the sharing of offices by lawyers precludes one of those who so shares with another from accepting a case which the other cannot ethically accept. To a considerable degree, that opinion relied upon informal opinions previously published by the American Bar Association's Standing Committee on Professional Ethics.

Since the publication of Opinion 75-13, the question has been considered by the appropriate committees on many state bar associations. The written opinions range from being flatly prohibitive to generally permissive.

The discussions generally relate to two Canons. Canon 4 requires the preservation of confidences and secrets of clients. Canon 9 requires the avoidance of even the appearance of professional impropriety.

A sampling of the various state opinions follows:

Alabama - The adverse representation is permitted where the two lawyers share a secretarial pool, a conference room, a library, and other common areas of the building, provided that the lawyers do not have access to each other's files in matters in which they represent opposing interests.

Illinois - Adverse representation is permitted where the lawyers share office space and secretarial help. Such representation is permitted so long as each lawyer

discloses the potential and conflicting situation to the clients, and obtains the client's consent, and each lawyer can represent his client with undivided allegiance. The lawyers, however, may not share a common secretary in the representation of clients with adverse interests. Such practice creates the potential for disclosure of confidential information and the appearance of impropriety.

Indiana - Lawyers who share office space, telephone systems, reception area, and a library in the same building may represent adverse parties in the same case if there is no access between the telephone systems of the separate practices, the reception area is arranged such that one lawyer's secretary is not able to overhear confidences from another lawyer's clients, case materials are not left in the copier area or library, and clients are informed of the space sharing arrangement and the measures undertaken to avoid any compromise of confidentiality.

Iowa - An attorney who practices criminal law may not share an office with two part-time county attorneys. The public may believe that the criminal attorney holds special influence over the office of the prosecuting attorney. Further, the arrangement creates an opportunity to imply that the prosecutors have access to the lawyer's files and to information concerning the lawyer's clients.

Kentucky - A lawyer who shares offices with the county attorney may not accept employment adverse to the county nor defend criminal cases in any other county. Since the county attorney may not defend cases in any other county or federal court, neither may a partner, associate or person who shares office space with the county attorney practice criminal law in those jurisdictions. The appearance of impropriety is too great.

Maine - A lawyer who maintains a separate law practice but shares office space, equipment, and personnel with another lawyer may not represent a client in an action against a client of the other lawyer.

The mutual sharing arrangement may Jeopardize both client's confidences.

Michigan - Lawyers who share office space may represent clients with potential conflicting interests provided certain protective measures are taken. The lawyers must establish office procedures that will assure that client's confidences and secrets are maintained. For example, the responsible lawyer may store client files in a locked desk or in his home so as not to risk accidental compromise should either lawyer chance upon them in the general office area. Each lawyer must fully explain the relationship to his clients, indicate that there will be no compromise of confidences, and obtain the consent of the client to continue representation.

Missouri - Lawyers may share an office and represent opposing parties so long as they hold themselves out as maintaining separate practices and no confidential information is passed between them. However, sharing a common secretary could pose problems.

New Hampshire - A county attorney may not conduct his civil law practice from an office shared with criminal defense lawyers. The possibility of breaches of confidentiality has a chilling effect on a defendant's disclosure of confidential information and creates the appearance of impropriety as the close proximity of the offices may suggest to the public that the defense attorneys are in a position to influence the conduct of the county attorney.

New York City - Law firms may not represent opposing parties where the two firms share a suite of offices, and where the two firms have close working relationship (i.e. the two firms act as co-counsel in some cases, refer cases to each other, share a telephone system, and the secretaries of both law firms cover for one another). There is a strong likelihood that confidences and secrets of the firms' respective clients cannot be maintained. The relationship between office sharing lawyers places an undue burden upon each attornev to maintain the client's confidences and

secrets.

North Carolina - Lawyers who share office space may represent conflicting interests if the confidentiality of each lawyer's practice is maintained in both appearance and fact. The lawyers may share a common library and copying equipment, for example, but not a common telephone number or lay personnel.

Vermont - Two attorneys may occupy adjacent offices and share a library, conference room and office equipment, and yet represent clients with conflicting interests. In such an arrangement, the attorneys are not subject to the same conflict of interest restrictions as attorneys who are affiliated as partners. However, sharing of files, secretarial coverage and discussion would invite an implication of impropriety. To avoid misunderstandings, the attorneys should inform their clients of the separateness of attorneys.

Virginia - Two attorneys sharing office space and a secretary must withdraw from the representation of clients that are adverse, unless consent of clients is obtained after full disclosure. Clients who are infants are not capable of providing the informed consent necessary to rectify a conflict of interest.

In addition to the foregoing, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued Informal Opinion 1486 on February 8, 1982. This opinion is as follows:

> The committee is asked whether a lawyer may rent space from a law firm where the lawyer and the law firm represent adverse interests in pending lawsuits and contemplate referrals to each other in the future. The lawyer will not be associated with the law firm in any way except that the lawyer will rent an office from the law firm and will share with the law firm a reception area, secretarial space and library facilities. The lawyer will use separate stationery and will not be listed on the law firm stationery.

> The lettering on the door will indicate the existence of two separate law practices.
>
> In the opinion of the committee, if the lawyer complies in good faith with the requirements of DR 4-101 and DR 5-101 (A), the lawyer and the law firm may make the arrangement described above. DR 4 1-1 requires that the lawyer exercise reasonable care to prevent the lawyer's employees and associates, as well as others whose services are utilized by the lawyer, from disclosing or using confidences or secrets of a client. The lawyer and the law firm should be particularly sensitive to this requirement and establish office procedures that will assure that confidence or secrets are maintained. The lawyer and the law firm also should explain fully the relationship to, and obtain the consent of, their clients to continue to represent adverse interests in the pending lawsuits and to represent adverse interests in future matters.

After carefully considering each of the foregoing opinions and the rationales thereof, as well as the economic realities of today's solo practice, we are persuaded that Opinion No. 75-13 should be modified.

We now hold that lawyers who maintain separate and independent practices but share certain office facilities, including reception area, conference rooms, library, computer systems and receptionist and secretarial personnel, may represent adverse parties so long as the following precautions are met:

1. There shall be no common access to the case files;

2. There shall be no common access to any computerized data relating to the case;

3. No secretary shall be allowed to

work on the case for both parties;

4. All common employees shall be informed of the adverse representation and the extreme sensitivity to the maintenance of confidentiality; and

5. Each client shall give his/her consent to the adverse representation after full disclosure of all facts relating to the common practice area.

It must be stressed that while these rules may not always be easy to apply and enforce, they are extremely important to avoid the appearance of impropriety.

CONCLUSION

Lawyers who maintain separate and independent practices but share certain office facilities, including reception area, conference rooms, library, computer systems, and receptionist and secretarial personnel, may represent adverse parties so long as the following precautions are met:

1. There shall be no common access to the case files;

2. There shall be no common access to any computerized data relating to the case;

3. No secretary shall be allowed to work on the case for both parties;

4. All common employees shall be informed of the adverse representation and the extreme sensitivity to the maintenance of confidentiality; and

5. Each client shall give his/her consent to the adverse representation after full disclosure of all facts relating to the common practice area.

Nebraska Ethics Advisory Opinion for Lawyers
No. 89-2

Nebraska Ethics Advisory Opinion for Lawyers
No. 88-3

IT IS NOT POSSIBLE TO STATE A DEFINITE TIME AS TO WHEN CLOSED CLIENT FILES MAY BE DESTROYED. THE RETENTION OR DESTRUCTION OF CLIENT FILES IS PRIMARILY A MATTER OF GOOD JUDGMENT, WEIGHING THE CLIENTS' INTERESTS AND EXPECTATIONS IN THE RETENTION OF FILE MATERIALS, THE REASONABLY EXPECTED FUTURE USEFULNESS OF THE FILE CONTENTS, THE CAREFUL PRESERVATION OF CONFIDENTIALITY, AND THE AVAILABILITY OF STORAGE SPACE.

QUESTION PRESENTED

How long must an attorney keep a closed client file before destroying it?

DISCUSSION

DR 9-102 (B) of the Code of Professional Responsibility as adopted by the Nebraska Supreme Court clearly establishes the duty upon lawyers to maintain inviolate the ownership of property belonging to clients.

The Committee has reviewed Opinion CI-22 of the Committee on Professional and Judicial Ethics of the State Bar of Michigan, Opinion 74 of the Maine Board of Bar Overseers Professional Ethics Committee, and Formal Opinion 1986-4 of the Association of the Bar of the City of New York. The thrust of these opinions, with which this Committee concurs, is that no general rule can be fashioned setting forth a specific period of time after which it is safe to destroy a client's file.

An attorney does not have a duty to preserve permanently all of his files. Mounting and substantial storage costs can raise the cost of legal services, and the public interest is not served by unnecessary and avoidable cost increases. Clients and former clients, on the other hand, have a right to expect that valuable

information in their lawyers' files, not otherwise available to them, will not be carelessly destroyed.

The following are suggested guidelines to assist the attorney in making the decision as to the retention or destruction of client files:

1. The file may include original documents or other property furnished by or on behalf of the client, the return of which might reasonably be expected by the client. Before destroying such documents or property, the client should be asked whether he wants delivery of them. Alternatively, the lawyer may simply deliver such documents to the client with appropriate advice regarding factors which the client should consider in determining which items to preserve. Where unable to contact the client, the lawyer should be guided by the foreseeable need for the documents in determining whether to destroy them.

2. An attorney must use care not to destroy or discard information that he knows or should know may still be necessary or useful in the assertion or defense of the client's position in a matter for which a statute of limitations has not expired.

3. An attorney must consider the reasonable expectations of the client for the preservation of files.

4. The nature and contents of some files may indicate a need for longer retention than do the nature and contents of other files, based upon their relevance and materiality to matters that can be expected to arise in the future.

5. Disposition of client files must be made in such a manner as to protect fully the confidentiality of the contents.

It should also be noted that an attorney should retain indefinitely accurate and complete records of all receipts and disbursements of trust funds.

CONCLUSION

It is not possible to state a definite time as to when closed client files may be destroyed. The retention or destruction of client files is primarily a matter of good judgment, weighing the clients' interests and expectations in the retention of file materials, the reasonably expected future usefulness of the file contents, the careful preservation of confidentiality, and the availability of storage space.

Nebraska Ethics Advisory Opinion for Lawyers
No. 88-3

Wisconsin Formal Ethics Opinion EF-15-01:
Ethical Obligations of Attorneys Using Cloud Computing

March 23, 2015

Synopsis

A lawyer may use cloud computing as long as the lawyer uses reasonable efforts to adequately address the risks associated with it. The Rules of Professional Conduct require that lawyers act competently to protect client information and confidentiality as well as to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed.

To be reasonable, the lawyer's efforts must be commensurate with the risks presented. Among the factors to be considered in assessing that risk are the information's sensitivity; the client's instructions and circumstances; the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party; the attorney's ability to assess the technology's level of security; the likelihood of disclosure if additional safeguards are not employed; the cost of employing additional safeguards; the difficulty of implementing the safeguards; the extent to which the safeguards adversely affect the lawyer's ability to represent clients; the need for increased accessibility and the urgency of the situation; the experience and reputation of the service provider; the terms of the agreement with the service provider; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

To determine what efforts are reasonable, lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground. Lawyers should also understand the dangers of using public Wi-Fi and file sharing sites. Lawyers who outsource cloud computing services should understand the importance of selecting a provider that uses appropriate security protocols. Lawyers should also understand the importance of regularly backing up data and storing data in more than one place. A lawyer may consult with someone who has the necessary knowledge to help determine what efforts are reasonable.

Introduction

Technology has dramatically changed the practice of law in many ways, including the ways in which lawyers process, transmit, store, and access client information. Perhaps no area has seen greater change than "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."[1] In other words, cloud computing includes the processing, transmission, and storage of the client's information using shared computer facilities or remote servers owned or leased by a third-party service provider.[2] These facilities and services are accessed over the Internet by the lawyer's networked devices such as computers, tablets, and smart phones.[3]

Many lawyers welcome cloud computing as a way to reduce costs, improve efficiency, and provide better client service. The cloud service provider assumes responsibility for infrastructure, application software, development platforms, developer and programming staff, licensing, updates, security and maintenance, while the lawyer enjoys access to the client information from any location that has Internet access. Along with the lawyer's increased accessibility comes the loss of direct control over the client's information. The provider of cloud computing adds a layer of risk between the lawyer and client's information because most of the physical, technical, and administrative safeguards are managed by the cloud service provider. Yet the ultimate responsibility for insuring the confidentiality and security of the client's information lies with the lawyer.

As cloud computing becomes more ubiquitous and as clients demand more efficiency, the question for counsel is no longer whether to use cloud computing, but how to use cloud computing safely and ethically. Lawyers may disagree about how to balance the competing risks of security breaches and provider outages, on the one hand, and the convenience of access and protection from natural or local disasters, on the other. Yet, whatever decision a lawyer makes must be made with reasonable care, and the lawyer should be able to explain what factors were considered in making that decision.

Ethics opinions from other states that have addressed the issue of cloud computing have generally concluded that a lawyer may use cloud computing if the lawyer uses reasonable efforts to adequately address the risks in doing so.[4] But the definition of what is reasonable varies.

The State Bar's Standing Committee on Professional Ethics (the "Committee") agrees with the conclusion of ethics opinions from other states that cloud computing is permissible as long as the lawyer uses reasonable efforts to adequately address the potential risks associated with it. Part I of this opinion

---

[1] Pennsylvania Bar Ass'n Comm. on Legal Ethics and Professional Responsibility Formal Ethics Opinion 2011-200 (2011), at 1 (quoting Quinn Norton, "Byte Rights," *Maximum PC,* September 2010, at 12). A more detailed definition is difficult to formulate because cloud computing is not a single system, but includes different technologies, configurations, service models, and deployment models. For example, cloud computing encompasses web-based email, online data storage, software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). Deployment models include public clouds, private clouds, hybrid clouds, and managed clouds.

[2] "These remote servers may be hosted in data centers worldwide, allowing cloud service providers to distribute computing power, storage capacity and data across their data centers dynamically to provide fast delivery and on-demand bandwidth." Stuart D. Levi and Kelly C. Riedel, "Cloud Computing: Understanding the Business and Legal Issues," *Practical Law,* http://us.practicallaw.com/8-501-5479

[3] The National Institute of Standards and Technology defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Wayne Jansen & Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, Special Publication # 800-145 (September 2011). Almost any information technology or computing resource can be delivered as a cloud service.

[4] Appendix A to this opinion provides a brief description of the ethics opinions from other states.

identifies the specific rules of Wisconsin's Rules of Professional Conduct for Attorneys that are implicated by cloud computing and the duties imposed by those rules. Part II of this opinion discusses what constitutes reasonable efforts to protect the lawyer's access to and the confidentiality of client information.

Part I: The Applicable Rules

Several rules are implicated by the use of cloud computing. These rules are SCR 20:1.1 Competence, SCR 20:1.4 Communication, SCR 20:1.6 Confidentiality, and SCR 20:5.3 Responsibilities regarding nonlawyer assistants.

A. SCR 20:1.1 Competence

SCR 20:1.1 requires a lawyer to perform legal services competently.[5] ABA Comment [8] to Model Rule 1.1, amended in 2012, recognizes that technology is an integral part of contemporary law practice and explicitly reminds lawyers that the duty to remain competent includes keeping up with technology.

> [8] 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Moreover, ABA Comment [5] recognizes that competency also requires the "use of methods and procedures meeting the standards of competent practitioners."

Lawyers who use cloud computing have a duty to understand the use of technologies and the potential impact of those technologies on their obligations under the applicable law and under the Rules. In order to determine whether a particular technology or service provider complies with the lawyer's professional obligations, a lawyer must use reasonable efforts. Moreover, as technology, the regulatory framework, and privacy laws change, lawyers must keep abreast of the changes.

B. SCR 20:1.4 Communication

SCR 20:1.4(b) requires that a lawyer explain a matter to the extent reasonably necessary to permit the client to make informed decisions concerning the representation.[6] While it is not necessary for a

---

[5] SCR 20:1.1 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.

[6] SCR 20:1.4 Communication

(a) A lawyer shall:

(1) Promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in SCR 20:1.0(f), is required by these rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests by the client for information; and

lawyer to communicate every detail of a client's representation, the client should have sufficient information to participate intelligently in decisions concerning the objectives of representation and the means by which they are to be pursued.[7] Of concern is whether a lawyer must inform the client of the means by which the lawyer processes, transmits, and stores the client's information in all representations or only when the circumstances call for it, such as where the information is particularly sensitive.

None of the ethics opinions have suggested that a lawyer is required in all representations to inform the client of the means by which the lawyer processes, transmits, and stores information. One ethics opinion, however, suggests that a lawyer should consider giving notice to the client about the proposed method for storing client information.[8] Yet, lawyers' remote storage of client information is not a new occurrence: lawyers have been using off-site brick-and-mortar storage facilities for many years. Another opinion suggests that "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."[9]

While none of the ethics opinions have suggested that a client's informed consent is required in all instances before a lawyer may use cloud computing, one opinion has suggested that client consent may be necessary to use a third-party service provider when the information is highly sensitive.[10] If consent is required, SCR 20:1.4(a)(1) requires that the lawyer promptly inform the client.

The Committee agrees with other ethics opinions that a lawyer is not required in all representations to inform the client that the lawyer uses the cloud to process, transmit or store information. SCR 20:1.4 does not require the lawyer to inform the client of every detail of representation. It does, however, require the lawyer to provide the client with sufficient information so that the client is able to meaningfully participate in his or her representation. "The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation."[11]

While a lawyer is not required in all representations to inform clients that the lawyer uses the cloud to process, transmit or store information, a lawyer may choose, based on the needs and expectations of the clients, to inform the clients. A provision in the engagement agreement or letter is a convenient way to provide clients with this information.

---

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

[7] SCR 20: 1.4 ABA Comment [5].

[8] Vt. Ethics Op. 2010-6 (2011) at 7.

[9] Pa. Ethics Op. 2011-200 at 6.

[10] N.H. Ethics Op. 2012-13/4 at 2.

[11] SCR 20:1.4 ABA Comment [5] (2012).

If there has been a breach of the provider's security that affects the confidentiality or security of the client's information, SCR 20:1.4(a)(3) and SCR 20:1.4(b) require the lawyer to inform the client of the breach.

C. SCR 20:1.6 Confidentiality

The duty to protect information relating to the representation of the client is one of the most significant obligations imposed on the lawyer. SCR 20:1.6(a) prohibits a lawyer from revealing information relating to the representation of a client unless that client gives informed consent or unless the disclosure is impliedly authorized in order to carry out the representation.[12] The processing, transmission, and storage of information in the cloud may be deemed an impliedly authorized disclosure to the provider as long as the lawyer takes reasonable steps to ensure that the provider of the cloud computing services has adequate safeguards.[13]

Although a lawyer has a professional duty to protect information relating to the representation of the client from unauthorized disclosure, this duty does not require any particular means of handling protected information and does not prohibit the employment of service providers who may handle documents or data containing protected information. Lawyers are not required to guarantee that a breach of confidentiality cannot occur when using a cloud service provider, and they are not required to use only infallibly secure methods of communication.[14] They are, however, required, to use reasonable efforts to protect information relating to the representation of their clients from unauthorized disclosure.

The 2012 revision of ABA Model Rule 1.6 and its Comment made "clear that a lawyer has an ethical duty to take reasonable measures to protect a client's confidential information from inadvertent disclosure, unauthorized disclosure, and unauthorized access, regardless of the medium used."[15] A new

---

[12] The provisions in SCR 20:1.6(b) and (c) are not implicated in cloud computing.

SCR 20:1.6 Confidentiality

(a) A lawyer shall not reveal information relating to the 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 pars. (b) and (c).

(b) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal or fraudulent act that the lawyer reasonably believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interest or property of another.

(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably likely death or substantial bodily harm;

(2) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(3) to secure legal advice about the lawyer's conduct under these rules;

(4) to establish a claim or defense on behalf of the lawyer in a 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; or

(5) to comply with other law or a court order.

[13] Pa. Ethics Op. 2011-200 at 6.

[14] A.B.A. Comm'n on Ethics 20/20 *Introduction & Overview,* at 8 (August 2012).

[15] A.B.A. Comm'n on Ethics 20/20 *Introduction & Overview,* at 8 (August 2012).

paragraph was added to Model Rule 1.6 stating that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[16]

Moreover, the 2012 revision of ABA Comment [18] to Model Rule 1.6 emphasizes that unauthorized access to or the inadvertent or unauthorized disclosure of information relating to the representation of a client does not constitute a violation of the rule "if the lawyer has made reasonable efforts to prevent the access or disclosure." The comment identifies a number of factors to be considered in determining the reasonableness of the lawyer's efforts. 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)."[17]

---

[16] Model Rules of Prof'l Conduct R. 1.6(c) (2012). The numbering for SCR 20:1.6 differs from the Model Rule 1.6 because Wisconsin retains in our paragraph (b) the mandatory disclosure requirements that have been a part of the Wisconsin Supreme Court Rules since their initial adoption. SCR 20:1.6(c) contains the discretionary disclosure requirements. Wisconsin Committee Comment to SCR 20:1.6.

[17] ABA Comment [18] to Model Rule 1.6 states:

> Acting Competently to Preserve Confidentiality
>
> [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and 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. 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 paragraph (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. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

Similarly, the 2012 revision of ABA Comment [19] requires a lawyer, when transmitting a communication that includes information relating to the representation of the client, to take reasonable precautions to prevent the information from coming into the hands of unintended recipients. ABA Comment [19] to Model Rule 1.6 states:

> [19] 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

A lawyer using cloud computing may encounter circumstances that require unique considerations to secure client confidentiality. For example, if a server used by a cloud service provider is physically located in another country, the lawyer must be sure that the data on that server are protected by laws that are as protective as those of the United States. Whether a lawyer is required to take additional precautions to protect 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.[18]

D. SCR 20:5.3 Responsibilities regarding nonlawyer assistants

Although a lawyer may use nonlawyers outside the firm to help provide legal services, SCR 20:5.3 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.[19] The extent of this obligation when using a cloud service provider to process, transmit, store, or access information protected by the duty of confidentiality will depend greatly on the experience, stability, security measures and reputation of the provider as well as the nature of the information relating to the representation of the client.

ABA Comment [3], added as part of the 2012 revisions, identifies distinct concerns that arise when services are performed outside the firm. It recognizes that nonlawyer services can take many forms, such as services performed by individuals and services performed by automated products. It identifies the factors that determine the extent of the lawyer's obligations when using such services, and it also references other Rules of Professional Conduct that the lawyer should consider when using such services. Comment [3] also emphasizes that the lawyer has an obligation to give appropriate instructions to nonlawyers outside the firm when retaining or directing those nonlawyers. For example, when a lawyer retains an investigative service, the lawyer may not be able to directly supervise how a particular investigator completes an assignment, but the lawyer's instructions must be reasonable under the circumstances to provide reasonable assurance that the investigator's conduct is compatible with the lawyer's professional obligations.[20]

---

[18] Model Rules of Prof'l Conduct R. 1.6 Comment [18] (2012).

[19] SCR 20:5.3 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; 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 knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

[20] ABA Comment [3] to Model Rule 5.3 states:

> [3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When

ABA Comment [4], also added as part of the 2012 revisions, recognizes that clients sometimes direct lawyers to use particular nonlawyer service providers.[21] In such situations, the Comment advises that the lawyer should ordinarily consult with the client to determine how the outsourcing arrangement should be structured and who will be responsible for monitoring[22] the performance of the nonlawyer services.

Part II: Reasonable Efforts

The Rules of Professional Conduct do not impose a strict liability standard on lawyers who use cloud computing, and none of the ethics opinions require extraordinary efforts or a guarantee that information will not be inadvertently disclosed or that the information will always be accessible when needed.[23] Instead, the Rules require that lawyers act competently to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed, as well as to protect client information from unauthorized access and disclosure, whether intentional or inadvertent. Competency requires the lawyer to make reasonable efforts; and to be reasonable, those efforts must be commensurate with the risk presented.

---

using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

[21] ABA Comment [4] to Model Rule 5.3 states:

> [4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

[22] The ABA Commission on Ethics 20/20 acknowledged that the word "monitoring" reflects "a new ethical concept," but concluded that the new concept was needed because it may not be possible for the lawyer to "directly supervise" a nonlawyer when the nonlawyer is performing the services outside the firm. Report to the House of Delegates Resolution 105C, Report p. 8. The word "monitoring" makes it clear that the lawyer has an obligation to remain aware of how nonlawyer services are being performed. The Comment also reminds lawyers that they have duties to tribunal that may not be satisfied through compliance with this Rule. For example, if a client instructs a lawyer to use a particular electronic discovery vendor, the lawyer cannot cede all monitoring responsibility to the client because the lawyer may have to make certain representations to the tribunal regarding the vendor's work. *Id.*

[23] As one ethics opinion stated: "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." N.J. Advisory Committee on Professional Ethics Op. No. 701 (2006).

What constitutes reasonable efforts has been the subject of much discussion. It has been suggested that some of the ethics opinions may place unrealistic demands on attorneys.[24] At the same time, it has been suggested that "[i]n sum, basic knowledge of cybersecurity has become an essential lawyer competency."[25]

This Committee agrees with other ethics opinions that lawyers cannot guard against every conceivable danger when using the cloud to process, transmit, store and access client information. This Committee concludes that lawyers must make reasonable efforts to protect client information and confidentiality as well as to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed. To be reasonable, those efforts must be commensurate with the risks presented. Because technologies differ and change rapidly, the risks associated with those technologies will vary. Moreover, because the circumstances of each law practice vary considerably, the risks associated with those law practices will also vary. Consequently, what may be reasonable efforts commensurate with the risks for one practice may not be for another. And even within a practice, what may be reasonable efforts for most clients may not be for a particular client.

A. Factors to Consider when Assessing the Risks

To be reasonable, the lawyer's efforts must be commensurate with the risks presented by the technology involved, the type of practice, and the individual needs of a particular client. The ABA in its Comments to Model Rules 1.6 and 5.3 as well as other ethics opinions have identified factors for lawyers to consider when assessing the risks. These factors, which are not exclusive, include:

- the information's sensitivity;[26]
- the client's instructions and circumstances;[27]

[24] One expert in the field of data security, Stuart L. Pardau, points out that some ethics opinions, such as Pennsylvania Ethics Op. 2011-200, direct attorneys to negotiate favorable terms of use with the cloud service providers, even though the opinions acknowledge that the providers' terms are usually "take it or leave it" and that a typical attorney is powerless to require a cloud provider to do anything beyond the boilerplate terms. Stuart L. Pardau, "But I'm Just a Lawyer: Do Cloud Ethics Opinions Ask Too Much?" The Professional Lawyer, Vol. 22, Number 4 2014. Pardau also notes that some opinions require attorneys to know information that they have no practical way of knowing. As examples, Pardau cites Nevada Formal Ethics Op. 33 (2006), which concludes that the attorney will not be responsible for a cloud service provider's breach of confidentiality if the attorney "instructs and requires the third party contractor to keep the information confidential and inaccessible," and New Hampshire Ethics Op. 2012-13/4 opinion, which advises that the attorney "must know at all times where sensitive client information is stored, be it in the cloud or elsewhere." Pardau further observes that "[s]ome of the state bar ethics opinions go too far in requiring attorneys to understand cloud security and monitor providers," citing Alabama Formal Ethics Op. 2010-02, which states that a lawyer has "a continuing duty to stay abreast of the appropriate safeguards that should be employed by … the third-party vendor."

[25] Andrew Perlman, "The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence" The Professional Lawyer, Vol. 22, Number 4 2014. Perlman, a law school professor who directs an institute on law practice technology, observes that lawyers "store a range of information in the 'cloud' (both private and public) as well as on the 'ground' using smartphones, laptops, tablets, and flash drives." He further observes that this "information is easily lost or stolen; it can be accessed without authority (e.g., through hacking); it can be inadvertently sent; it can be intercepted in transit; and it can be accessed without permission by foreign governments or the National Security Agency." He concludes that "[i]n light of these dangers, lawyers need to understand how to competently safeguard confidential information."

[26] ABA Model Rule 1.6 Comment [18]. The more sensitive the information, the less risk an attorney should take.

[27] Calif. Formal Ethics Op. 2010-179 (2010). A lawyer must follow the client's instructions unless doing so would cause the lawyer to violate the Rules of Professional Conduct or other law. Moreover, a lawyer should consider any circumstances that may be

- the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;[28]
- the attorney's ability to assess the technology's level of security;[29]
- the likelihood of disclosure if additional safeguards are not employed;[30]
- the cost of employing additional safeguards;[31]
- the difficulty of implementing the additional safeguards;[32]
- the extent to which the additional safeguards adversely affect the lawyer's ability to represent clients;[33]
- the need for increased accessibility and the urgency of the situation;[34]
- the experience and reputation of the service provider;[35]
- the terms of the agreement with the service provider;[36] and
- the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.[37]

---

relevant. For example, if the attorney is aware that other people have access to the client's devices or accounts and may intercept client information, the attorney should consider that in assessing the risk.

[28] ABA Model Rule 1.6 Comment [18].

[29] Calif. Formal Ethics Op. 2010-179 (2010). The opinion concludes:

> 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.

Similarly, Iowa Ethics Op. 11-01 (2011) concludes:

> 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 it own qualified employees.

[30] ABA Model Rule 1.6 Comment [18].

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Calif. Formal Ethics Op. 2010-179 (2010).

[35] ABA Model Rule 5.3 Comment [3].

[36] *Id.*

[37] *Id.*

Once the lawyer has assessed the risks by considering the various factors, the lawyer is able to determine what efforts are reasonable to protect against those risks.

B. General Guidance

It is impossible to provide specific requirements for reasonable efforts because lawyers' ethical duties are continually evolving as technology changes. Specific requirements would soon become obsolete. Moreover, the risks vary with the technology involved, the type of practice, and the individual needs of a particular client.[38] Lawyers must exercise their professional judgment in adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers, and specific requirements would do little to assist the exercise of professional judgment. It is possible, however, to provide some guidance.

- Lawyers should have "at least a base-level comprehension of the technology and the implications of its use."[39] While attorneys are not required to understand precisely how the technology works, competence requires at least a cursory understanding of the technology used. Such a cursory understanding is necessary to explain to the client the advantages and risks of using the technology in the representation.[40]

- Lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication,[41] and encryption for information stored both in the cloud and on the ground.[42] Lawyers should also understand the security dangers of using public Wi-Fi and file sharing sites.

- Lawyers who outsource cloud-computing services should understand the importance of selecting a provider that uses appropriate security protocols. "While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track record prior to utilizing the service."[43] Knowing the qualifications, reputation, and longevity of the cloud-service provider is necessary, just like knowing the qualifications, reputation, and longevity of any other service provider.

---

[38] For example, the efforts required of a lawyer whose practice is limited to patent law will vary from the efforts required of a lawyer whose practice is limited to family law because the risks presented by a patent law practice differ from risks presented by a family law practice. Even within the patent law practice, the efforts may vary depending on the needs of a particular client.

[39] Joshua H. Brand, "Cloud Computing Services – Cloud Storage," *Minnesota Lawyer* (01/01/2012) at 1. Accessed at http://www.docstoc.com/docs/117971742/Cloud-Computing-Services-_-Cloud-Storage-by-Joshua-H-Brand .

[40] *Id.*

[41] Multifactor authentication ensures that data can be accessed only if the lawyer has the correct password as well as another form of identification, such as a code sent by text message to the lawyer's mobile phone.

[42] "On the ground" refers to the use of smart phones, tablets, laptops, and flash drives.

[43] Brand at 2.

- Lawyers should read and understand the cloud-based service provider's terms of use or service agreement.[44]

- Lawyers should also understand the importance of regularly backing up data and storing data in more than one place.

- Lawyers who do not have the necessary understanding should consult with someone who has the necessary skill and expertise, such as a technology consultant, to help determine what efforts are reasonable.[45]
- Lawyers should also consider including a provision in their engagement agreements or letters that, at the least, informs and explains the use of cloud-based services to process, transmit, store and access information. Including such a provision not only gives the client an opportunity to object, but it also provides an opportunity for the lawyer and client to discuss the advantages and the risks.

---

[44] Lawyers should pay particularly close attention to the following terms:

> *Ownership of the Information*
> Do the terms of use specifically state that the provider has no ownership interest in the information? What happens to the information if the provider goes out of business or if the lawyer decides to terminate the business relationship, or if the lawyer defaults on payments?
> *Location of the Information*
> Where is information stored? Many providers replicate the information to data centers or servers in other countries with less stringent legal protections. What is the provider's response to government or judicial attempts to obtain client information?
> *Security and Confidentiality of Information*
> What safeguards does the provider have to prevent security breaches? What obligations does the provider have to protect the confidentiality of information? Does the provider agree to promptly notify the lawyer of known security breaches that affect the confidentiality of the lawyer's information?
> *Service Level*
> Does the service provider have an uptime guarantee? Most providers agree to a 99.9% uptime, although some providers agree to a higher uptime approaching 99.999%.
> *Backups*
> How frequently does the provider backup the information? How easy is it to restore the information from the backup?
> *Disaster Recovery*
> Does your provider have a secondary data center or redundant storage that automatically assumes control if disaster strikes the data center or server?

[45] Wa. Ethics Op. 2215 (2012) concludes:

> 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.

Similarly, the California ethics opinion acknowledges that an attorney need not "develop a mastery of the security features and deficiencies of each technology available," but advises that if an attorney lacks the expertise to evaluate cloud providers, "he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant." Calif. Formal Ethics Op. 2010-179. Likewise, the Arizona ethics opinion concludes that lawyers must "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." Ariz. Ethics Op. 09-04 (2009).

Conclusion

Ethics opinions from other states that have addressed the issue of cloud-based services have generally concluded that a lawyer may use cloud computing if the lawyer takes reasonable care in doing so. This Committee agrees with the opinions issued by other states that cloud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it. The Committee concludes that lawyers must make reasonable efforts to protect client information and confidentiality as well as to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed. To be reasonable, those efforts must be commensurate with the risks presented. Lawyers must exercise their professional judgment when adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers.

Appendix A
Cloud Ethics Opinions

Alabama
Alabama State Bar Disciplinary Commission
Ala. Ethics Op. 2010-02 (2010)
Lawyers may outsource the storage of client files through cloud computing if reasonable steps are taken to make sure the information is protected. Lawyers must be knowledgeable about how the data will be stored and its security, and must reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Lawyers must also stay abreast of security safeguards.

Arizona
State Bar of Arizona Committee on the Rules of Professional Conduct
Ariz. Ethics Op. 09-04 (2009)
Lawyers may use an online file storage and retrieval system that enables clients to access their files as long as the lawyers take reasonable precautions to protect the security and confidentiality of the information. Lawyers must "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." Lawyers must also periodically review the security measures. "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."

California
State Bar of California Standing Committee on Professional Responsibility and Conduct
Calif. Formal Ethics Op. 2010-179 (2010)
A lawyer's duties of confidentiality and competence require the lawyer to take appropriate steps to ensure that his or her use of technology does not subject client information to an undue risk of unauthorized disclosure. Among the factors to be considered are the technology's level of security, the information's sensitivity, the urgency of the matter, the possible effect inadvertent disclosure or unauthorized interception could pose to a client or third party, as well as client instructions and circumstances.

> 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. 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.

Connecticut

Connecticut Bar Association Professional Ethics Committee
Conn. Informal Ethics Op. 2013-07(2013)

A "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." The Professional Ethics Committee acknowledged that although the technology examined by it in 1999 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." As concluded by the 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."

Florida

The Florida Bar Professional Ethics Committee
Fla. Ethics Op. 12-3 (2013)

Relying on the New York State Bar Ethics Opinion 842 (2010) and Iowa Ethics Opinion 11-10 (2011), the opinion concludes that 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. Lawyers should research the service provider used and also consider backing up the data elsewhere as a precaution.

Iowa

Iowa State Bar Association Committee on Ethics and Practice Guidelines
Iowa Ethics Op. 11-01 (2011)

The opinion concludes that the lawyer is obligated "to perform due diligence to assess the degree of protection that will be needed and to act accordingly." The opinion gives basic guidance by listing questions that the lawyer should ask:

Accessibility

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 Obligations:*
   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 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

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 that others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?

The opinion recognizes that performing due diligence can be complex and requires specialized knowledge and skill. The opinion also acknowledges that a law firm may discharge the duties "by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees."

Maine
Maine State Bar Association Professional Ethics Committee
Maine Ethics Op. 194 (2008)
Lawyers may use third-party electronic back-up and transcription services as long as appropriate safeguards are taken, including reasonable efforts to prevent the disclosure of confidential information, and an agreement with the vendor that contains "a legally enforceable obligation" to maintain the confidentiality of the client's information.

Massachusetts
Massachusetts Bar Association Committee on Professional Ethics
Mass. Ethics Op. 12-03 (2012)
A lawyer may generally store and synchronize electronic work files containing client information across different platforms and devices using the Internet as long as the lawyer undertakes reasonable efforts to ensure that the provider's terms of use, privacy policies, practices and procedures are compatible with the Lawyer's professional obligations. Reasonable efforts would include:

(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 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).

The lawyer should follow the client's express instructions regarding the use of cloud technology to store and transmit data; and for particularly sensitive client information, the lawyer should obtain client approval before using cloud technology to store or transmit the information.

Nevada

State Bar of Nevada Standing Committee on Ethics and Professional Responsibility
Nev. Formal Ethics Op. 33 (2006)

A lawyer may store client files electronically on a remote server controlled by a third party as long as the firm takes reasonable precautions, such as obtaining the third party's agreement to maintain confidentiality, to prevent both accidental and unauthorized disclosure of confidential information.

New Hampshire

New Hampshire Bar Association Ethics Committee
N.H. Ethics Op. 2012-13/4 (2013)

A lawyer may use cloud computing consistent with his or her ethical obligations, as long as the lawyer takes reasonable steps to ensure that client information remains confidential. The opinion lists ten issues the lawyer must consider: (1) whether the provider is a reputable organization; (2) whether the provider offers robust security measures; (3) whether the data is stored in a retrievable format; (4) whether the provider commingles data belonging to different clients or different lawyers; (5) whether the provider has a license and not an ownership interest in the data; (6) whether the provider has an enforceable obligation to keep the data confidential; (7) whether the servers are located in the United States; (8) whether the provider will retain the data, and for how long, when representation ends or the agreement between the lawyer and the provider terminates; (9) whether the provider is required to notify the lawyer if the information is subpoenaed, if the law permits such notice; and (10) whether the provider has a disaster recovery plan with respect to the data.

New Jersey

Advisory Committee on Professional Ethics (appointed by the Supreme Court of New Jersey)
N.J. Ethics Op. 701 (2006)

When using electronic filing systems, lawyers must exercise reasonable care against unauthorized access. "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."

New York

New York State Bar Association Committee on Professional Ethics
N.Y. State Bar Ethics Op. 842 (2010)

A lawyer may use an online computer data storage system to store client files provided "the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained." Reasonable care includes "(1) ensuring that the provider has enforceable obligations 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 (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." In addition, the lawyer should stay informed of both technological advances that could affect confidentiality and changes in the law that could affect any privilege protecting the information.

North Carolina

North Carolina State Bar Ethics Committee
N.C. Formal Ethics Op. 2011-6 (2012)

"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." The opinion, however, recommends some security measures.

- 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 the 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-propriety 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.
- Evaluation of the extent to which the SaaS vendor backs up hosted data.

The opinion also encourages law firms to consult periodically with professionals competent in the area of online security because of the rapidity with which computer technology changes.

Ohio

Ohio State Bar Association Professionalism Committee

Ohio State Bar Association Informal Advisory Op. 2013-03

"[A] lawyer's duty 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 information." When selecting a vendor, it is necessary for the lawyer to know the qualifications, reputation, and longevity of the vendor, and to read and understand the agreement entered into with the vendor. The opinion lists the following "commonly-occurring issues":

- 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?
- 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 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?

Consistent with other ethics opinions, such as those from Pennsylvania and New Hampshire, the opinion concludes that storing client data in the cloud does not always require prior consultation because it interprets the language "reasonably consult" as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation.

Oregon

Oregon State Bar Legal Ethics Committee

Or. Ethics Op. 2011-88

A lawyer "may store client materials on a third-party server as long as the lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation." Reasonable steps to ensure that the vendor will reliably secure client data and keep information confidential "may include, among other things, ensuring the service agreement requires the vendor to preserve confidentiality and security of the materials. It may also require that vendor notify the lawyer of any nonauthorized third-party access to the materials." Moreover, the lawyer "may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials" because as "technology advances, the third-party vendor's protective measures may become less secure or obsolete over time."

Pennsylvania
Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility
Pa. Ethics Op. 2011-200
A lawyer "may ethically allow client confidential material to be stored in 'the cloud' provided the lawyer 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." The opinion advises that "[l]awyers may need to consider that at least some data may be too important to risk inclusion in cloud services." The opinion contains a list of over 30 precautions that reasonable care may require.

Vermont
Vermont Bar Association
Vt. Advisory Ethics Op. 2010-6 (2011)
Lawyers may use cloud computing in connection with client information as long as they take reasonable precautions to protect the confidentiality of and to ensure access to the information. "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 the 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."

Virginia
Virginia Bar Association Standing Committee on Legal Ethics
Va. Legal Ethics Op. 1872 (2013)
"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 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." Virginia's Rule 1.6(b)(6) provides that to the extent a lawyer reasonably believes necessary, the lawyer may reveal "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."

Washington

Washington State Bar Association Rules of Professional Conduct Committee

Wa. Ethics Op. 2215 (2012)

This opinion suggests that the best practices for lawyers "without advanced technological knowledge" would 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 about cloud computing industry standards and features. (2) Evaluation of the provider's practices, reputation, and history. (3) Comparison of provisions in the 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."