(/)

2. Counselor Related Opinions (/Ethics/EthicsOpinions/RelatedOpinions?id=7)

ER 2.1. Advisor

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

Comment

Scope of Advice

[1] A client is entitled to straightforward advice expressing the lawyer's honest assessment. Legal advice often involves unpleasant facts and alternatives that a client may be disinclined to confront. In presenting advice, a lawyer endeavors to sustain the client's morale and may put advice in as acceptable a form as honesty permits. However, a lawyer should not be deterred from giving candid advice by the prospect that the advice will be unpalatable to the client.

[2] Advice couched in narrowly legal terms may be of little value to a client, especially where practical considerations, such as cost or effects on other people, are predominant. Purely technical legal advice, therefore, can sometimes be inadequate. It is proper for a lawyer to refer to relevant moral and ethical considerations in giving advice. Although a lawyer is not a moral advisor as such, moral and ethical considerations impinge upon most legal questions and may decisively influence how the law will be applied.

[3] A client may expressly or impliedly ask the lawyer for purely technical advice. When such a request is made by a client experienced in legal matters, the lawyer may accept it at face value. When such a request is made by a client inexperienced in legal matters, however, the lawyer's responsibility as advisor may include indicating that more may be involved than strictly legal considerations.

[4] Matters that go beyond strictly legal questions may also be in the domain of another profession. Family matters can involve problems within the professional competence of psychiatry, clinical psychology or social work; business matters can involve problems within the competence of the accounting profession or of financial specialists. Where consultation with a professional in another field is itself something a competent lawyer would recommend, the lawyer should make such a recommendation. At the same time, a lawyer's advice at its best often consists of recommending a course of action in the face of conflicting recommendations of experts.

Offering Advice

[5] In general, a lawyer is not expected to give advice until asked by the client. However, when a lawyer knows that a client proposes a course of action that is likely to result in substantial adverse legal consequences to the client, the lawyer's duty to the client under ER 1.4 may require that the lawyer offer advice if the client's course of action is related to the representation. Similarly, when a matter is likely to involve litigation, it may be necessary under ER 1.4 to inform the client of forms of dispute resolution that might constitute reasonable alternatives to litigation. A lawyer ordinarily has no duty to initiate investigation of a client's affairs or to give advice that the client has indicated is unwanted, but a lawyer may initiate advice to a client when doing so appears to be in the client's interest.

(/)

Member Login Search

1. Client-Lawyer Relationship

Related Opinions (/Ethics/EthicsOpinions/RelatedOpinions?id=32)

ER 1.13. Organization as Client

(a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances, to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in paragraph (d), if

(1) despite the lawyer's efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action or refusal to act, that is clearly a violation of law, and

(2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization, then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

(d) Paragraph (c) shall not apply with respect to information relating to a lawyer's representation of an organization to investigate an alleged violation of law, or to defend the organization or an officer, employee or other constituent associated with the organization against a claim arising out of an alleged violation of law.

(e) A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraphs (b) or (c), or who withdraws under circumstances that require or permit the lawyer to take action under either of those paragraphs, shall proceed as the lawyer reasonably believes

necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

(f) In dealing with an organization's directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization's interests are adverse to those of the constituents with whom the lawyer is dealing.

(g) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of ER 1.7. If the organization's consent to the dual representation is required by ER 1.7, the consent shall be given by an appropriate official of the organization other than the individual who is to be represented, or by the shareholders.

Comment

The Entity as the Client

[1] An organizational client is a legal entity, but it cannot act except through its officers, directors, employees, shareholders and other constituents. Officers, directors, employees and shareholders are the constituents of the corporate organizational client. The duties defined in this Comment apply equally to unincorporated associations. "Other constituents" as used in this Comment means the positions equivalent to officers, directors, employees and shareholders held by persons acting for organizational clients that are not corporations.

[2] When one of the constituents of an organizational client communicates with the organization's lawyer in that person's organizational capacity, the communication is protected by ER 1.6. Thus, by way of example, if an organizational client requests its lawyer to investigate allegations of wrongdoing, interviews made in the course of that investigation between the lawyer and the client's employees or other constituents are covered by ER 1.6. This does not mean, however, that constituents of an organizational client are the clients of the lawyer. The lawyer may not disclose to such constituents information relating to the representation except for disclosures explicitly or impliedly authorized by the organizational client in order to carry out the representation or as otherwise permitted by ER 1.6.

[3] When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonable necessary in the best interest of the organization. As defined in Rule 1.0 (f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[4] In determining how to proceed under paragraph (b), the lawyer should give due consideration to the seriousness of the violation and its consequences, the responsibility in the organization and the apparent motivation of the person involved, the policies of the organization concerning such matters, and any other relevant considerations. Ordinarily, referral to a higher authority would be necessary. In some circumstances, however, it may be appropriate for the lawyer to ask the constituent to reconsider the matter; for example, if the circumstances involve a constituent's innocent misunderstanding of law and subsequent acceptance of the lawyer's advice, the lawyer may reasonably conclude that the best interest of the organization does not require that the matter be referred to higher

authority. If a constituent persists in conduct contrary to the lawyer's advice, it will be necessary for the lawyer to take steps to have the matter reviewed by a higher authority in the organization. If the matter is of sufficient seriousness and importance or urgency to the organization, referral to higher authority in the organization may be necessary even if the lawyer has not communicated with the constituent. Any measures taken should, to the extent practicable, minimize the risk of revealing information relating to the representation outside the organization. Even in circumstances where a lawyer is not obligated by Rule 1.13 to proceed, a lawyer may bring to the attention of an organizational client, including its highest authority, matters that the lawyer reasonably believes to be of sufficient importance to warrant doing so in the best interests of the organization.

[5] Paragraph (b) also makes clear that when it is reasonably necessary to enable the organization to address the matter in a timely and appropriate manner, the lawyer must refer the matter to higher authority, including, if warranted by the circumstances, the highest authority that can act on behalf of the organization under applicable law. The organization's highest authority to whom a matter may be referred ordinarily will be the board of directors or similar governing body. However, applicable law may prescribe that under certain conditions the highest authority reposes elsewhere, for example, in the independent directors of a corporation.

Relation to Other Rules

[6] The authority and responsibility provided in this Rule are concurrent with the authority and responsibility provided in other Rules. In particular, this Rule does not limit or expand the lawyer's responsibility under ERs 1.8, 1.16, 3.3 or 4.1. Paragraph (c) of this Rule supplements Rule 1.6(d) by providing an additional basis upon which the lawyer may reveal information relating to the representation, but does not modify, restrict, or limit the provisions of Rule 1.6(d)(1)-(5). Under paragraph (c) the lawyer may reveal such information only when the organization's highest authority insists upon or fails to address threatened or ongoing action that is clearly a violation of law, and then only to the extent the lawyer reasonably believes necessary to prevent reasonably certain substantial injury to the organization. It is not necessary that the lawyer's services be used in furtherance of the violation, but it is required that the matter be related to the lawyer's representation of the organization. If the lawyer's services are being used by an organization to further a crime or fraud by the organization. Rules 1.6(d)(1) and 1.6(d)(2) may permit the lawyer to disclose confidential information. In such circumstances Rule 1.2(d) may also be applicable, in which event, withdrawal from the representation under Rule 1.16(a)(1) may be required.

[7] Paragraph (d) makes clear that the authority of a lawyer to disclose information relating to a representation in circumstances described in paragraph (c) does not apply with respect to information relating to a lawyer's engagement by an organization to investigate an alleged violation of law or to defend the organization or an officer, employee or other person associated with the organization against a claim arising out of an alleged violation of law. This is necessary in order to enable organizational clients to enjoy the full benefits of legal counsel in conducting an investigation or defending against a claim.

[8] A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraph (b) or (c), or who withdraws in circumstances that require or permit the lawyer to take action under either of these paragraphs, must proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

Government Agency

[9] The duty defined in this Rule applies to governmental organizations. Defining precisely the identity of the client and prescribing the resulting obligations of lawyers may be more difficult in the government context. See Scope [18]. Although in some circumstances the client may be a specific agency, it may also be a branch of government, such as the executive branch, or the government as a whole. For example, if the action or failure to act involves the head of a bureau, either the department of which the bureau is a part or the relevant branch of government may be the client for purposes of this Rule. Moreover, in a matter involving the conduct of government officials, a government lawyer may have authority to question such conduct more extensively than that of a lawyer for a private organization in similar circumstances. Thus, when the client is a governmental organization, a different balance may be appropriate between maintaining confidentiality and assuring that the wrongful act is prevented or rectified, for public business is involved. In addition, duties of lawyers employed by the government or lawyers in military service may be defined by statutes and regulation. This Rule does not limit that authority. See Scope. Government lawyers also may have authority to represent the "public interest" in circumstances where a private lawyer would not be authorized to do so.

[10] A government lawyer may have an obligation to render advice to a government entity and constituents of a government entity.Normally, the government entity, rather than an individual constituent, is the client. Some government lawyers may also be elected officials or the employees of elected officials who have statutory obligations to take formal action against individual constituents under certain circumstances. The government lawyer, therefore, must clearly identify the client and disclose to the individual constituents any limitations that are imposed on the lawyer's other legal obligations. See ER 1.2(c) and related comments. Further, where a conflict arises between a constituent and the government entity the lawyer represents or between constituents of the same government entity, the lawyer must make the identity of the client clear to the constituents and determine which constituent has authority to act for the government entity in each instance.

Clarifying the Lawyer's Role

[11] There are times when the organization's interests may be or become adverse to those of one or more of its constituents. In such circumstances the lawyer should advise any constituent, whose interest the lawyer finds adverse to that of the organization of the conflict or potential conflict of interest, that the lawyer cannot represent such constituent, and that such person may wish to obtain independent representation. Care must be taken to assure that the individual understands that, when there is such adversity of interest, the lawyer for the organization cannot provide legal representation for that constituent individual, and that discussions between the lawyer for the organization and the individual may not be privileged.

[12] Whether such a warning should be given by the lawyer for the organization to any constituent individual may turn on the facts of each case.

Dual Representation

[13] Paragraph (e) recognizes that a lawyer for an organization may also represent a principal officer or major shareholder.

Derivative Actions

[14] Under generally prevailing law, the shareholders or members of a corporation may bring suit to compel the directors to perform their legal obligations in the supervision of the organization. Members of unincorporated associations have essentially the same right. Such an action may be brought nominally by the organization, but usually is, in fact, a legal controversy over management of the organization.

[15] The question can arise whether counsel for the organization may defend such an action. The proposition that the organization is the lawyer's client does not alone resolve the issue. Most derivative actions are a normal incident or an organization's affairs, to be defended by the organization's lawyer like any other suit. However, if the claim involves serious charges of wrongdoing by those in control of the organization, a conflict may arise between the lawyer's duty to the organization and the lawyer's relationship with the board. In those circumstances, ER 1.7 governs who should represent the directors and the organization.

(/)

4. Transactions with Persons Other Than Clients

Related Opinions (/Ethics/EthicsOpinions/RelatedOpinions?id=11)

ER 4.1. Truthfulness in Statements to Others

In the course of representing a client a lawyer shall not knowingly:

(a) make a false statement of material fact or law to a third person; or

(b) fail to disclose a material fact when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by ER 1.6.

Comment

Misrepresentation

[1] A lawyer is required to be truthful when dealing with others on a client's behalf, but generally has no affirmative duty to inform an opposing party of relevant facts. A misrepresentation can occur if the lawyer incorporates or affirms a statement of another person that the lawyer knows is false. Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements. For dishonest conduct that does not amount to a false statement or for misrepresentations by a lawyer other than in the course of representing a client, see ER 8.4.

Statements of Fact

[2] This Rule refers to statements of fact. Whether a particular statement should be regarded as one of fact can depend on the circumstances. Under generally accepted conventions in negotiation, certain types of statements ordinarily are not taken as statements of material fact. Estimates of price or value placed on the subject of a transaction and a party's intentions as to an acceptable settlement of a claim are ordinarily in this category, and so is the existence of an undisclosed principal except where nondisclosure of the principal would constitute fraud. Lawyers should be mindful of their obligations under applicable law to avoid criminal and tortious misrepresentation.

Crime or Fraud by Client

[3] Under ER 1.2(d), a lawyer is prohibited from counseling or assisting a client in conduct that the lawyer knows is criminal or fraudulent. Paragraph (b) states a specific application of the principle set forth in ER 1.2(d) and addresses the situation where a client's crime or fraud takes the form of a lie or misrepresentation. Ordinarily, a lawyer can avoid assisting a client's crime or fraud by withdrawing from the representation. Sometimes it may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm an opinion, document, affirmation or the like. In extreme cases, substantive law may require a lawyer to disclose information relating to the representation to avoid being deemed to have assisted the client's crime or fraud. If the lawyer can avoid assisting a client's crime or fraud only by disclosing this information, then under paragraph (b) the lawyer is required to do so, unless the disclosure is prohibited by ER 1.6. If disclosure is permitted by ER 1.6, then such disclosure is required under this Rule, but only to the extent necessary to avoid assisting a client crime or fraud.

The 14 General Principles of Ethical Conduct

5 C.F.R §2635.101 (b)

The following general principles apply to every employee and may form the basis for the standards contained in this part. Where a situation is not covered by the standards set forth in this part, employees shall apply the principles set forth in this section in determining whether their conduct is proper.

1. Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain.
2. Employees shall not hold financial interests that conflict with the conscientious performance of duty.
3. Employees shall not engage in financial transactions using nonpublic Government information or allow the improper use of such information to further any private interest.
4. An employee shall not, except as permitted by subpart B of this part, solicit or accept any gift or other item of monetary value from any person or entity seeking official action from, doing business with, or conducting activities regulated by the employee's agency, or whose interests may be substantially affected by the performance or nonperformance of the employee's duties.
5. Employees shall put forth honest effort in the performance of their duties.
6. Employees shall not knowingly make unauthorized commitments or promises of any kind purporting to bind the Government.
7. Employees shall not use public office for private gain.
8. Employees shall act impartially and not give preferential treatment to any private organization or individual.
9. Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.
10. Employees shall not engage in outside employment or activities, including seeking or negotiating for employment, that conflict with the official Government duties and responsibilities.

11. Employees shall disclose waste, fraud, abuse, and corruption to the appropriate authorities.
12. Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those—such as Federal, State, or local taxes—that are imposed by law.
13. Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age, or handicap.
14. Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part. Whether particular circumstances create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the relevant facts.

The principles of ethical conduct were issued by George H. W. Bush, In Executive Order 12674, as amended by Executive Order 12731. The principles were subsequently issued in the *Standards of Ethical Conduct for Employees of the Executive Branch* at 5C.F.R. § 2635.101(b). Each executive branch agency has a Designated Agency Ethics Officer responsible for oversight of the agency's ethics program.

ADOT
CODE OF CONDUCT

A letter from our Director, John Halikowski

Dear Fellow Employees:

The foundation of ADOT's success rests in its values. We all understand that regardless of the circumstances we are all accountable for upholding the Department's good reputation.

Regardless of the times we live in, all of us are trying to accomplish more in less time, with shrinking resources. The task of balancing all of life's challenges can be enormous, but so are the opportunities. Given ADOT's operating environment, temptations to engage in actions that depart from ADOT's values will occur.

ADOT's Code of Conduct is based on three values: **Integrity, Respect** and **Accountability**. While these articulate our values and beliefs, the Code itself provides guidance to ensure we meet those standards and adhere to those values.

The Code consists of the following sections:

- Interactions with customers and Stakeholders
- Contract Related Activities
- Conflicts of Interest and Personal Gain or Benefit
- Use of ADOT Resources
- Outside Business Interests
- Political Activity
- Equal Employment Opportunities
- Compliance

The complete Code of Conduct follows this letter.

I expect all employees to conduct themselves in a manner that will not discredit or embarrass the department; It is essential that we protect the reputation of the Arizona Department of Transportation. Adhering to the Code of Conduct is a condition of employment at ADOT. All employees need to understand the Code and are required to apply its standards in their every day responsibilities.

We all benefit from maintaining a good reputation. I thank you all for assisting me in doing so.

John S. Halikowski

THE ADOT CODE OF CONDUCT

Although the Code may not cover every situation, it does set forth a basic philosophy of conducting business. Employees are encouraged to seek the advice of their immediate supervisor if they are in doubt about any situation, potential decision or action. More specific guidelines may be available to employees of individual business sections to help them apply the Code in particular work areas.

Interaction with Customers and Stakeholders

ADOT employees and representatives are expected to be honest, fair and objective when communicating with customers and stakeholders. We are committed to satisfying our customers and partners by delivering quality products and services.

This means that ADOT employees and representatives must never:

- make false or misleading statements
- engage in deceptive or unfair practices
- engage in activities that may be perceived to be dishonest, deceptive or unfair

Contract Related Activities

Employees who deal with outside contractors must maintain independence and impartiality in their business relationships, both in fact, as well as in appearance. ADOT will not tolerate illegal or unethical business practices. All decisions shall be based on an impartial assessment of the costs and benefits to ADOT.

This means that ADOT employees and representatives must:

- not give or receive gifts, gratuities, or entertainment in exchange for business favors or to influence a business decision.
- avoid personal relationships that can be construed as conflicts of interest or raise the appearance of impropriety.
- adhere to the ADOT Gift Policy and other procurement related policies and restrictions.

Conflicts of Interest and Personal Gain or Benefit

All employees have a responsibility to act in the best interest of ADOT. Employees are prohibited from using their positions for personal benefit or gain. All employees need to avoid not only conflicts of interest, but the appearance of a conflict of interest.

Any ADOT employee having a personal (including a family or other close personal relationship), or financial stake in the outcome of a decision is required to reveal to their supervisor that relationship before being involved in the decision making.

Use of ADOT Resources

ADOT resources, (tangible assets such as equipment and tools; and intangible assets such as time and knowledge) are for ADOT business. It is the responsibility of each employee to ensure the proper use and protection of all ADOT resources. Employees

are expected to be familiar with and adhere to all ADOT policies including electronic equipment usage.

Outside Business Interests
Employees may choose to become involved in business interests outside ADOT. Situations that may have potential conflicts of interest should be discussed with your supervisor and be in accordance with ADOA Rule R2-5-501 Standards of Conduct, and ADOT PER-6.02 Conflict of Interest of Officers and Employees and Secondary Employment.

Political Activity
All employees are expected to adhere to the provisions of ARS 41-770 Causes for Dismissal or Discipline, regarding political activity, as well as the ADOT Policy on Political Activity PER-6.01.

Equal Employment Opportunities
ADOT is committed to a policy of nondiscrimination. ADOT employees at all levels do not discriminate against any individual on the basis of race, color, sex, religion, national origin, age, pregnancy and/or disability.

Personnel decisions should be made based on merit. These decisions include hiring, promotions, discipline, transfer, recruitment, advertising, reduction in force, all compensation, selection for training, job assignments, accessibility, working conditions, special duty details, and employee evaluations.

Compliance with ADOT's Code of Conduct
Employees who violate ADOT's Code of Conduct put themselves and the agency at the risk of facing serious legal consequences, including criminal penalties. Code of Conduct violations will result in disciplinary action, up to and including termination.

Periodically, all ADOT employees will be required to take a training course and will be asked to sign a document stating that you understand and are in compliance with the Code of Conduct, and have disclosed all situations that may present a conflict of interest.

ARIZONA DEPARTMENT OF TRANSPORTATION
POLICIES AND PROCEDURES

PER-6.02 CONFLICT OF INTEREST OF OFFICERS AND EMPLOYEES

2.01 PURPOSE

To familiarize Arizona Department of Transportation (ADOT) officers and employees, including newly-hired employees, with the (1) State's conflict of interest laws, (2) ADOT's policy related to conflict of interest, (3) the State's Standards of Conduct, and (4) ADOT's Code of Conduct.

2.02 SCOPE

A. This chapter summarizes the conflict of interest laws, which establishes minimum standards for the conduct of public officers and employees who are, or may become, involved with a contract or decision in their official capacity which might affect their personal pecuniary interest or those of their relatives, i.e., spouse, children, grandchildren, parent, grandparent, brother, sister and their spouses, or the parent, brother, or sister or child of one's spouse.

B. "Interest", as described in the conflict of interest laws, refers to a pecuniary, financial, or property interest by which a public officer, employee, and/or relative, stands to gain.

C. Public officers are defined under the State's conflict of interest laws as all elected and appointed officers of a public agency (such as the State Transportation Board, MAG employee, ADOT Director, etc.), whereas employees are defined as anyone employed by an incorporated city or town, political subdivision of the State, the State, or any of its departments, commissions, agencies, bodies, or boards for compensation, whether on a full-time, part-time, or contract basis.

2.03 AUTHORITY

Authority for this policy is provided by Arizona Revised Statute (A.R.S.) § 38-501 through A.R.S. § 38-511, Conflict of Interest of Officers and Employees, and by Section R-2-5-501 of the Arizona Department of Administration Personnel Rules (Exhibit 1).

2.04 DEFINITIONS

See Exhibit 2 – A.R.S. § 38-502 Definitions.

2.05 BACKGROUND

This policy was formerly titled Conflict of Interest of Officers and Employees and Secondary Employment. The sections related to Secondary Employment were removed and placed into a new policy, PER-6.07, Secondary Employment, on March 13, 2009.

2.06 THE ARIZONA CONFLICT OF INTEREST LAW

A. **Impact** - The Arizona conflict of interest law affects ADOT and its officers and employees in the following manner:

1. A conflict of interest potentially arises whenever a public officer or employee of ADOT has, or whose relative has, a substantial interest in *any contract with, sale to, purchase from, or service provided* to ADOT. When such an interest exists, a public officer or employee shall make known that interest in writing to ADOT, and shall refrain from voting upon or otherwise participating in any manner as an officer or employee regarding such contract, sale, purchase or service.

2. A conflict of interest also potentially arises whenever a public officer or employee of ADOT has, or whose relative has, a substantial interest in any *decision* of ADOT. When such an interest exists, a public officer or employee shall make known that interest in writing to ADOT, and shall refrain from participating in any manner as an officer or employee in such decision.

3. Notwithstanding the provisions of section 2.05 A. 1. and 2. above, no public officer or employee of ADOT shall supply to ADOT any equipment, material, supplies, or services, *unless* pursuant to an award or contract let after public competitive bidding.

B. **Substantial Interest** - To determine whether a substantial interest exists, the public officer or employee must ask the following questions:

1. Will the contract, sale, purchase, service, or decision have an impact, either positive or negative, on an interest of him/herself or a relative?

2. Is the interest pecuniary or proprietary? (A pecuniary interest involves money; a proprietary interest involves ownership.)

3. Is the interest other than one statutorily designated as a remote interest? See Section 2.06 C.

If the answer to any of these questions is yes, then a substantial interest exists which requires disclosure and disqualification by the public officer or employee. See Section 2.06 D.

Thus, although the officer or employee may not have a substantial interest in a decision in which he is about to participate, if one of his relatives has a substantial interest in the decision, he /she must disclose the interest and refrain from participating in the decision. See Section 2.06 D. He/she may not justify his/her failure to comply with the conflict of interest laws by stating he/she was unaware of his/her relative's interest. Public officers and employees have an affirmative obligation to become aware of any interests their relatives may have in which they may become involved.

C. **Remote Interests** - A.R.S. § 38-502 (11), Exhibit 2, excludes from the definition of a substantial interest ten enumerated remote interests, A.R.S. § 38-502(10) (a to i). Any interest in a decision or contract not covered by one or more of the enumerated remote interests is a substantial interest requiring compliance with the disclosure and withdrawal requirements of the law.

D. **Compliance** - The officer or employee must be aware of and identify the circumstances in which an agency's actions might affect the interests of himself or his relatives and avoid any situation in which a conflict of interest exists. Once a determination is made that the interest is a substantial and not a remote interest, disclosure of that interest and withdrawal from participation is mandatory. Even if the public officer or employee believes that he/she can be objective in the matter and that the public interest would not be harmed by his/her participation, he/she must both disclose the conflict and completely withdraw from consideration of the matter in which his/her interests are involved. Disclosure and

disqualification must occur even if there is little or no likelihood that the officer or employee would participate in the matter.

Arizona's conflict of interest statutes are broadly construed in favor of the public and, substantial civil and criminal penalties are provided for failure to comply with the statutory requirements.

1. **Disclosure of Interest** - A.R.S. § 38-509, requires that all state agencies "maintain for public inspection in a special file, all documents necessary to memorialize" disclosures of potential conflicts of interests. Any public officer or employee who has a conflict of interest in any agency decision or in the award of a contract must disclose that interest in the special conflict of interest file of the public agency, A.R.S. § 38-503(A)(B). The officer or employee may either file a signed written disclosure statement fully disclosing the interest or file a copy of the official minutes of the agency which fully discloses the interest, A.R.S. § 38-502(3) and § 38-509.

2. **What To Do If You May Have A Conflict of Interest: Specific Disclosure and Blanket Disclosure** - Any officer or employee who feels that he/she may have a conflict of interest in a specific matter should immediately disqualify himself from participation in all related activities and decisions and prepare a memorandum, directed to the officer's or employee's supervisor, explaining in detail the conflict of interest and affirming that the officer or employee has disqualified himself. This memorandum will be placed in the conflict of interest file maintained by the agency for public inspection pursuant to A.R.S. § 38-509. The officer or employee should identify the specific matter in which there may be a substantial interest based on whatever knowledge he/she possesses.

   Having disclosed the conflict of interest and disqualified himself, the officer or employee must not communicate about the matter with anyone involved in the decision making process in order to avoid the appearance of impropriety.

3. **Rule of Impossibility** - In the unlikely situation that the majority of members of an agency have a conflict of interest and the agency is unable to act in its official capacity, A.R.S. § 38-508(B) provides the members may participate in the agency's decision after making known their conflict of interest in the official records of their public agency.

4. **Representation of Others** - A.R.S. § 38-504(A) states: " No public officer or employee may represent another person for compensation before a public agency by which he is or was employed within the preceding twelve months or on which he serves or served within the preceding twelve months concerning any matters with which such officer or employee was directly concerned and in which he personally participated during his employment or service by a substantial and material exercise of administrative discretion."

5. **Disclosure or Use of Information Declared Confidential by Law** - Current and former public officers and employees are prohibited from disclosing or using, without appropriate authorization, any information designated confidential by statute or rule, acquired by them in the course of their official duties. A.R.S. § 38-504(B).

6. **Disclosure or Use of Information Designated Confidential by Agency Action** - A.R.S. 38-504(B) prohibits a public officer or employee from disclosing or using for profit information acquired in the course of official duty which is designated as confidential, other than by statute or rule, and which he/she obtained from his/her agency as a result of his employment or service with the agency. The prohibition exists during the course of employment and for two years after employment has terminated, unless appropriate authorization from his/her agency has been obtained.

The prohibition includes either the disclosure or use of the information. Thus, even though no personal profit inures to the benefit of the public officer or employee through its use, he still is prohibited from disclosing the information for the statutory period.

7. **Improper Use of Office for Personal Gain** - A.R.S. § 38-504(C) prohibits public officers and employees from using or attempting to use their official position in order to secure valuable benefits for themselves, unless such benefits are part of the compensation they would normally be entitled to for performing their duties.

8. **Receiving Additional Income for services** - A.R.S. § 38-505(A) prohibits a public officer or employee from agreeing to receive or receiving, either directly or indirectly, compensation other than as provided by law for services rendered by him/her in any case, proceeding, application or other matter pending before his/her agency.

E. **Sanctions for Violations**

1. **Criminal Penalties** - The knowing or intentional violation of any provision of the conflict of interest of law is a class 6 felony, A.R.S. § 38-510(A)(1).

The negligent or reckless violation of the law is a class 1 misdemeanor. This means that a public officer or employee may be prosecuted if he fails to disclose a conflict of interest, of which he did not, but should have known, A.R.S. § 38-510 (A)(2).

The knowing falsification, concealment, or cover-up of a material fact pursuant to a scheme to defraud in any matter related to the business conducted by a state agency or any political subdivision of the state is a class 5 felony, A.R.S. § 13-2311.

2. **Forfeiture of Public Office** - Upon conviction of a violation of the conflict of interest laws, a public officer or employee forfeits his public office or employment, A.R.S. § 38-510(B).

3. **Contract Cancellation** - Any contract made by the state or any of its departments or agencies is subject to cancellation by the Governor if anyone significantly involved in the contract process on behalf of the state was or is also employed by or acted as consultant to any other party to the contract during the time the contract or extension to the contract is in effect, A.R.S. § 38-511.

2.07 ADOT'S CONFLICT OF INTEREST POLICY

A. It is ADOT policy to encourage all its officers and employees to become thoroughly familiar with A.R.S. § 38-502 to § 511 and to not violate the intent of these statutes while conducting official business. In addition, ADOT has specifically developed the following policy, based on A.R.S. § 38-502 and § 503, concerning the business conduct of officers and employees. (For secondary employment rules and procedures, see ADOT Policy and Procedure PER-6.07, Secondary Employment.)

B. The officers or employees shall not affiliate themselves with public or private organizations or entities so as to raise an expectation that official favors will be granted.

1. No officer or employee shall accept or solicit, directly or indirectly, anything of economic value which is or may appear to be designed to influence official conduct, particularly from persons seeking to obtain contractual, business or other financial arrangements with the Department or who has interests that might be substantially affected by the performance of the officer's or employee's duty.

2. Officers or employees should exercise caution when accepting meals, beverages or other refreshments from individuals who are seeking or already conducting official business with the state. The acceptance of beverages or other incidental refreshments should be limited to the infrequent occasions when offered in the ordinary course of a meeting or conference, and when such foods are offered at no charge to all participants.

3. This policy does not restrict an officer or employee from seeking a loan from a financial institution on customary terms and for proper purposes, nor does it prohibit the acceptance of unsolicited promotional materials of nominal value.

4. Since the intention of this policy is to avoid even the appearance of any impropriety, officers or employees are encouraged to report any offer of a gift or gratuity to the immediate supervisor as soon as possible after such an offer is made.

2.08 PROCEDURE FOR REPORTING SUBSTANTIAL INTERESTS OF OFFICERS OR EMPLOYEES AND RELATIVES

A. Arizona law requires that public officers and employees make known the existence of any substantial interest which they and their relatives have in:

1. Any contract, sale, purchase, or service to ADOT, and

2. Any decision to be made by ADOT.

B. Officers or employees shall submit a memorandum to his/her supervisor with the following information:

1. The nature of the substantial interest of the officer or employee or relative.

2. The contract sale, purchase, service or agency decision to which the substantial interest applies.

3. The name, address and telephone number of the relative.

4. The name, address and telephone number of the entity or persons involved in the contract, sale purchase, service or decision by ADOT.

5. A statement that the officer or employee will refrain from participating in any manner in the contract, sale purchase, service or decision by ADOT.

C. A copy of the memorandum shall be forwarded to the ADOT Human Resources Office to be placed in a special conflict of interest file maintained for public inspection.

2.08 CORRESPONDING POLICIES

A. Arizona Administrative Code (A.A.C.), Title 2, Chapter 5 (the State Personnel Rules).

B. A.R.S. § 38-501 through 511.

C. ADOT Code of Conduct.

D. ADOT Policy and Procedure PER-6.07, Secondary Employment.

R2-5-501. Standards of Conduct

A. General. In addition to statutorily prohibited conduct, including but not limited to A.R.S. § 41-770, a violation of the standards of conduct listed in subsections (B), (C), and (D) is cause for discipline or dismissal of a state service employee.

B. Required conduct. A state service employee shall at all times:;

1. *Maintain high standards of honesty, integrity, and impartiality, free from personal considerations, favoritism, or partisan demands;*
2. *Be courteous, considerate, and prompt in dealing with and serving the public and other employees;*
3. *Conduct himself or herself in a manner that will not bring discredit or embarrassment to the state; and*
4. *Comply with federal and state laws and rules, and agency policies and directives.*

C. Prohibited conduct. A state service employee shall not:

1. *Use his or her official position for personal gain, or attempt to use, or use, confidential information for personal advantage;*
2. *Permit himself or herself to be placed under any kind of personal obligation that could lead a person to expect official favors;*
3. *Perform an act in a private capacity that may be construed to be an official act;*
4. *Accept or solicit, directly or indirectly, anything of economic value as a gift, gratuity, favor, entertainment, or loan that is, or may appear to be, designed to influence the employee's official conduct. This provision shall not prohibit acceptance by an employee of food, refreshments, or unsolicited advertising or promotional material of nominal value;*
5. *Directly or indirectly use or allow the use of state equipment or property of any kind, including equipment and property leased to the state, for other than official activities unless authorized by written agency policy or as otherwise allowed by these rules;*
6. *Engage in outside employment or other activity that is not compatible with the full and proper discharge of the duties and responsibilities of state employment, or that tends to impair the employee's capacity to perform the employee's duties and responsibilities in an acceptable manner; or*
7. *Inhibit a state employee from joining or refraining from joining an employee organization.*

D. Employee rights. An employee shall not take disciplinary or punitive action against another employee that impedes or interferes with that employee's exercise of any right granted under the law or these rules. An employee or agency representative who is found to have acted in reprisal toward an employee as a result of the exercise of the employee's rights is subject to discipline, under Title 2, Chapter 5, Article 8. The discipline shall be administered in accordance with state and federal laws affecting employee rights and benefits.

Exhibit 1

A.R.S. § 38-502. Definitions

In this article, unless the context otherwise requires:

1. "Compensation" means money, a tangible thing of value or a financial benefit.
2. "Employee" means all persons who are not public officers and who are employed on a full-time, part-time or contract basis by an incorporated city or town, a political subdivision or the state or any of its departments, commissions, agencies, bodies or boards for remuneration.
3. "Make known" means the filing of a paper which is signed by a public officer or employee and which fully discloses a substantial interest or the filing of a copy of the official minutes of a public agency which fully discloses a substantial interest. The filing shall be in the special file established pursuant to section 38-509.
4. "Official records" means the minutes or papers, records and documents maintained by a public agency for the specific purpose of receiving disclosures of substantial interests required to be made known by this article.
5. "Political subdivision" means all political subdivisions of the state and county, including all school districts.
6. "Public agency" means:
   (a) All courts.
   (b) Any department, agency, board, commission, institution, instrumentality or legislative or administrative body of the state, a county, an incorporated town or city and any other political subdivision.
   (c) The state, county and incorporated cities or towns and any other political subdivisions.
7. "Public competitive bidding" means the method of purchasing defined in title 41, chapter 4, article 3, or procedures substantially equivalent to such method of purchasing, or as provided by local charter or ordinance.
8. "Public officer" means all elected and appointed officers of a public agency established by charter, ordinance, resolution, state constitution or statute.
9. "Relative" means the spouse, child, child's child, parent, grandparent, brother or sister of the whole or half blood and their spouses and the parent, brother, sister or child of a spouse.
10. "Remote interest" means:
   (a) That of a nonsalaried officer of a nonprofit corporation.
   (b) That of a landlord or tenant of the contracting party.
   (c) That of an attorney of a contracting party.
   (d) That of a member of a nonprofit cooperative marketing association.
   (e) The ownership of less than three per cent of the shares of a corporation for profit, provided the total annual income from dividends, including the value of stock dividends, from the corporation does not exceed five per cent of the total annual income of such officer or employee and any other payments made to him by the corporation do not exceed five per cent of his total annual income.
   (f) That of a public officer or employee in being reimbursed for his actual and necessary expenses incurred in the performance of official duty.
   (g) That of a recipient of public services generally provided by the incorporated city or town, political subdivision or state department, commission, agency, body or board of which he is a public officer or employee, on the same terms and conditions as if he were not an officer or employee.
   (h) That of a public school board member when the relative involved is not a dependent, as defined in section 43-1001, or a spouse.
   (i) That of a public officer or employee, or that of a relative of a public officer or employee, unless the contract or decision involved would confer a direct economic benefit or detriment upon the officer, employee or his relative, of any of the following:
      (i) Another political subdivision.
      (ii) A public agency of another political subdivision.
      (iii) A public agency except if it is the same governmental entity.
   (j) That of a member of a trade, business, occupation, profession or class of persons consisting of at least ten members which is no greater than the interest of the other members of that trade, business, occupation, profession or class of persons.
11. "Substantial interest" means any pecuniary or proprietary interest, either direct or indirect, other than a remote interest.

Exhibit 2

In addition to the prohibitions discussed herein, federal employees in the following agencies, divisions, or positions are "further-restricted" under the Hatch Act and cannot take an active part in political management or political campaigns (i.e., engage in political activity in concert with a political party, candidate for partisan political office, or partisan political group):

- Election Assistance Commission
- Federal Election Commission
- Office of the Director of National Intelligence
- Central Intelligence Agency
- Defense Intelligence Agency
- National Geospatial Intelligence Agency
- National Security Agency
- National Security Council
- National Security Division (DOJ)
- Criminal Division (DOJ)
- Federal Bureau of Investigation
- Secret Service
- Office of Criminal Investigation (IRS)
- Office of Investigative Programs (Customs)
- Office of Law Enforcement (ATF)
- Merit Systems Protection Board
- U.S. Office of Special Counsel
- Career members of the Senior Executive Service
- Administrative law judges, administrative appeals judges, and contract appeals board members.

For further examples, sample advisory opinions, and frequently asked questions, please visit our website at www.osc.gov.

Who We Are...

The U.S. Office of Special Counsel (OSC) is an independent federal investigative and prosecutorial agency. Our basic authorities come from four federal statutes: the Civil Service Reform Act, the Whistleblower Protection Act, the Hatch Act, and the Uniformed Services Employment & Reemployment Rights Act (USERRA).

OSC promotes compliance with the Hatch Act by providing advisory opinions about the law. Every year, OSC's Hatch Act Unit provides over a thousand advisory opinions, enabling individuals to determine whether their contemplated political activities are permitted under the Act. The Hatch Act Unit also enforces compliance with the Act by investigating alleged Hatch Act violations. Depending on the nature and severity of the violation, OSC may seek disciplinary action against an employee. OSC prosecutes Hatch Act violations before the Merit Systems Protection Board.

Contact Us:

U.S. Office of Special Counsel
1730 M Street, NW
Suite 218
Washington, DC 20036

Hatch Act Hotline:	(202) 254-3650 or (800) 854-2824
Hatch Act Fax:	(202) 254-3700
E-mail:	hatchact@osc.gov
Website:	www.osc.gov

U.S. OFFICE OF SPECIAL COUNSEL

A Guide to the Hatch Act for Federal Employees

September 2014

Understanding How the Hatch Act Applies to You

The Hatch Act generally applies to employees working in the executive branch of the federal government. The purpose of the Act is to maintain a federal workforce that is free from partisan political influence or coercion.

A Covered Employee:

- **May not** be a candidate for nomination or election to public office in a partisan election.
- **May not** use his or her official authority or influence to interfere with or affect the result of an election. For example:
  - > **May not** use his or her official title or position while engaged in political activity.
  - > **May not** invite subordinate employees to political events or otherwise suggest to subordinates that they attend political events or undertake any partisan political activity.
- **May not** knowingly solicit or discourage the participation in any political activity of anyone who has business before their employing office.
- **May not** solicit, accept, or receive a donation or contribution for a partisan political party, candidate for partisan political office, or partisan political group. For example:
  - > **May not** host a political fundraiser;
  - > **May not** invite others to a political fundraiser;
  - > **May not** sell tickets to a political fundraiser;
  - > **May not** use any e-mail account or social media to distribute, send, or forward content that solicits political contributions.
- **May not** engage in political activity — i.e., activity directed at the success or failure of a political party, candidate for partisan political office, or partisan political group — while the employee is on duty, in any federal room or building, while wearing a uniform or official insignia, or using any federally owned or leased vehicle. For example:
  - > **May not** distribute campaign materials;
  - > **May not** display campaign materials or items;
  - > **May not** perform campaign related chores;
  - > **May not** wear or display partisan political buttons, t-shirts, signs, or other items;
  - > **May not** make political contributions to a partisan political party, candidate for partisan political office, or partisan political group;
  - > **May not** post a comment to a blog or a social media site that advocates for or against a partisan political party, candidate for partisan political office, or partisan political group;
  - > **May not** use any e-mail account or social media to distribute, send, or forward content that advocates for or against a partisan political party, candidate for partisan political office, or partisan political group.

A Covered Employee:

- **May** be a candidate in a nonpartisan election.
- **May** register and vote as they choose.
- **May** assist in voter registration drives.
- **May** participate in nonpartisan campaigns.
- **May** contribute money to political campaigns, political parties, or partisan political groups.
- **May** attend political fundraising functions.
- **May** attend political rallies and meetings.
- **May** join political clubs or parties.
- **May** campaign for or against referendum questions, constitutional amendments, or municipal ordinances.
- **May** sign nominating petitions
- **May** circulate nominating petitions.*
- **May** campaign for or against candidates in partisan elections.*
- **May** make campaign speeches for candidates in partisan elections.*
- **May** distribute campaign literature in partisan elections.*
- **May** volunteer to work on a partisan political campaign.*
- **May** express opinions about candidates and issues. If the expression is political activity, however — i.e., activity directed at the success or failure of a political party, candidate for partisan political office, or partisan political group — then the expression is not permitted while the employee is on duty, in any federal room or building, while wearing a uniform or official insignia, or using any federally owned or leased vehicle.

* Further restricted employees, as described herein, may not engage in these activities.

What Happens if I Violate the Hatch Act?

An employee who violates the Hatch Act is subject to a range of disciplinary actions, including removal from federal service, reduction in grade, debarment from federal service for a period not to exceed 5 years, suspension, letter of reprimand, or a civil penalty not to exceed $1000.

An employee who violates these standards of conduct may be disciplined or separated from State employment.

Political Activities

Arizona Revised Statutes (A.R.S.) § 41-752 regulates the political activities of State officers and employees; the full text of this law is copied below:

A. Except for expressing an opinion or pursuant to section 16-402, an employee shall not engage in any activities permitted by this section while on duty, while in uniform or at public expense.

B. An employee shall not:

1. *Use any political endorsement in connection with any appointment to a position in the state personnel system.*
2. *Use or promise to use any official authority or influence for the purpose of influencing the vote or political action of any person or for any consideration.*

C. An employee, a member of the state personnel board or a member of the law enforcement merit system council shall not be a member of any national, state or local committee of a political party, an officer or chairperson of a committee of a partisan political club or a candidate for nomination or election to any paid public office, shall not hold any paid, elective public office or shall not take any part in the management or affairs of any political party or in the management of any partisan or nonpartisan campaign or recall effort, except that any employee may:

1. *Express an opinion.*
2. *Attend meetings for the purpose of becoming informed concerning the candidates for public office and the political issues.*
3. *Cast a vote and sign nomination or recall petitions.*
4. *Make contributions to candidates, political parties or campaign committees contributing to candidates or advocating the election or defeat of candidates.*
5. *Circulate candidate nomination petitions or recall petitions.*
6. *Engage in activities to advocate the election or defeat of any candidate.*
7. *Solicit or encourage contributions to be made directly to candidates or campaign committees contributing to candidates or advocating the election or defeat of candidates.*

D. A person shall not:

1. *Solicit any employee, member of the state personnel board or member of the law enforcement merit system council to engage or not engage in activities permitted by this section with the direct or indirect use of any threat, intimidation or coercion, including threats of discrimination, reprisal, force or any other adverse consequence, including the loss of any benefit, reward, promotion, advancement or compensation.*
2. *Subject any employee, member of the state personnel board or member of the law enforcement merit system council engaging in activity permitted by this section to any direct or indirect discrimination, reprisal, force, coercion or intimidation or any other adverse consequence, including the loss of any benefit, reward, promotion, advancement or compensation.*

3. *Subject any employee, member of the state personnel board or member of the law enforcement merit system council who chooses not to engage in any activity permitted by this section to any direct or indirect discrimination, reprisal, force, coercion or intimidation or any other adverse consequence, including the loss of any benefit, reward, promotion, advancement or compensation.*

E. *Subsections B and C of this section do not apply to those employees listed in section 41-742, subsection F.*

F. *This section does not apply to school board elections or community college district governing board elections, and an employee may serve as a member of the governing board of a common or high school district, as a member of a community college district governing board or in the office of precinct committeeman.*

G. *An employee who violates any of the provisions of this section is subject to suspension of not less than thirty days or dismissal.*

H. *A person who violates:*
   1. *Subsection D of this section is guilty of a class 6 felony.*
   2. *Any other provision of this section is guilty of a class 1 misdemeanor.*

I. *In addition to any other penalty, any person soliciting or encouraging a contribution in a manner prohibited by this section is subject to a civil penalty of up to three times the amount of the contribution solicited or encouraged plus costs, expenses and reasonable attorney fees.*

J. *This section does not deny any employee or board member any civil or political liberties as guaranteed by the United States and Arizona Constitutions.*

K. *It is the public policy of this state, reflected in this section, that government programs be administered in an unbiased manner and without favoritism for or against any political party or group or any member in order to promote public confidence in government, governmental integrity and the efficient delivery of governmental services and to ensure that all employees are free from any express or implied requirement or any political or other pressure of any kind to engage or not engage in any activity permitted by this section. Toward this end, any person or entity charged with the interpretation of this section shall take into account the policy of this section and shall construe any of its provisions accordingly.*

Conflict of Interest

Arizona Revised Statutes (A.R.S.) §§ 38-501 through 38-510 and State Personnel Rules place some restrictions with which employees must comply regarding business interests, outside (secondary) employment and employment of relatives. To ensure compliance with the provisions of these laws and rules, you are required to make an initial disclosure when first employed by the State and any time there is a change.

Work Hours

The state work week is the period of seven consecutive days starting Saturday at 12:00 a.m. and ending Friday at 11:59 p.m.

Operational needs vary from agency to agency, function to function and time to time. State agencies may require coverage 24 hours per day, seven days per week or only during usual business hours. There may be seasonal fluctuations or variations in workloads throughout the year based on the specific responsibilities of your agency.

F. Subsection B, paragraph 1 of this section, relating to open competition and subsection B, paragraph 4 of this section and subsection B, paragraph 5 of this section, relating to political affiliation, do not apply to:

1. Employees of the governor's office.

2. Employees of offices of elected officials who either:

(a) Report directly to the elected official.

(b) Head a primary component or report directly to the head of a primary component of the office of the elected official.

(c) As a primary duty, determine or publicly advocate substantive program policy for the office of the elected official.

3. The state agency head and each deputy director, or equivalent, of each state agency and employees of the state agency who report directly to either the state agency head or deputy director.

4. Each assistant director, or equivalent, of each state agency and employees in the state agency who report directly to an assistant director.

5. Attorneys in the office of the attorney general.

6. Employees in investment related positions in the state retirement system or plans established by title 38, chapter 5, article 2, 3, 4 or 6.

U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505
202-254-3600

Congress Allows Most State and Local Public Employees to Run for Partisan Office

On December 19, 2012, Congress passed the Hatch Act Modernization Act of 2012. The Act allows most state and local government employees to run for partisan political office. Prior to this change, state and local government employees were prohibited from running for partisan office if they worked in connection with programs financed in whole or in part by federal loans or grants. With the change, the federal Hatch Act no longer prohibits state and local government employees from running for partisan office unless the employee's salary is paid for completely by federal loans or grants.

This change will allow hundreds of thousands of state and local government employees to participate more actively in the democratic process in their communities.

Before entering a race as a candidate, employees should keep in mind the following:

- *Make sure your salary is not completely funded by federal loans or grants.* A very small number of state and local employees may continue to be prohibited from running for office by the federal Hatch Act. Before running for office, take steps to determine that your salary is not entirely -- 100% -- funded by federal loans or grants. Your state or local finance office should be able to clarify whether your salary is completely funded by federal loans or grants.

- *Make sure state or local law does not prohibit you from running.* Employees should also make sure that they are not prohibited from running for office by state or local law. Nearly every state, many localities, and the District of Columbia have ethics rules that govern the political activity of their employees. This includes, in some cases, the ability of employees to run for state or local office. While the rules under the federal Hatch Act have been relaxed with regard to partisan candidacies, states and localities are free to implement more rigid requirements at their discretion. OSC does not keep a comprehensive list of state and local political activity laws, and OSC does not enforce laws passed at the state or local level. Your state or local ethics office should be able to clarify whether any provision of state or local law prohibits you from running for office.

- *The Hatch Act restricts state or local employees from engaging in political misconduct.* The Hatch Act Modernization Act did not change the federal Hatch Act's prohibitions on coercive conduct or misuse of official authority for partisan purposes. A state or local employee is still covered by these prohibitions if the employee works in connection with a program financed in whole or in part by federal loans or grants, even if the connection is relatively minor. A covered employee who runs for office would violate the Hatch Act if the employee:
  - uses federal or any other public funds to support his own candidacy;
  - uses his state or local office to support his candidacy, including by using official email, stationery, office supplies, or other equipment or resources; or
  - asks subordinates to volunteer for his campaign or contribute to the campaign.

If you have questions about the Hatch Act or the Hatch Act Modernization Act, please call (800) 85-HATCH or (800) 854-2824, or write to hatchact@osc.gov.

2015-F-159

FORMAL ETHICS OPINION 2015-F-159

May an attorney ethically store confidential client information or material in "the cloud"?

OPINION

A lawyer may ethically allow confidential client information to be stored in "the cloud" if the lawyer takes reasonable care to assure that: (1) all such information or materials remain confidential; and (2) reasonable safeguards are employed to ensure that the information is protected from breaches, loss, and other risks. Due to rapidly changing technology, the Board doesn't attempt to establish a standard of care, but instead offers guidance from other jurisdictions.

DISCUSSION

Technological advances have changed the way lawyers and law firms may store, retrieve and access client information.An inquiry has been made regarding whether a lawyer can ethically store confidential client files and information in "the cloud".

Cloud computing is technology which allows a lawyer to store and access software or data through the cloud—a remote location which is not controlled by the lawyer but by a third party which provides the storage or other computing services. It is the use of a network of remote servers, hardware and/or software to store, manage, transmit, process and/or retrieve data off the lawyer's premises, rather than on a server or personal computer on the lawyer's premises.

The services, which may be long-term storage of confidential client information or shorter-term storage or services to enable data processing or web-based email, are typically purchased from a provider on a subscription fee basis. The service provider assumes the responsibility for new technology and software updates. The lawyer's computing device is simply a way of accessing the information stored in the cloud from any location with Internet access.[1]

Because cloud computing places data, including client data, on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable ethics rules. See "Cloud Ethics Opinions Around the U.S.", American Bar Association, Legal Technology Resource Center. This summary lists the standard of "reasonable care" with regard to the lawyer's use of cloud technology from all states supporting the use of cloud storage.

Due to the fact that technology is constantly evolving, this opinion only provides lawyers with guidance in the exercise of reasonable care and judgement regarding the lawyer's use of cloud technology in compliance with the rules of professional conduct, rather than mandating specific practices regarding the use of such technology. Ky. Ethics Op. E-437 (2014); Penn. Formal Ethics Op. 2011-200 (undated); Vt. Ethics Op. 2010-6 (2010).

Although cloud computing offers increased mobility and accessibility to client information, the placement of a service provider between the lawyer and confidential client information for which the lawyer is responsible adds a layer of risk and loss of direct control by the lawyer over the stored or transmitted information. N.H. Adv. Ethics Op. 2012-13/4 (2013). A lawyer owes the same ethical duties, obligations and protections to clients with respect to information for which they employ cloud computing as they otherwise owe clients pursuant to the Rules of Professional Conduct with respect to information in whatever form. Me. Ethics Op. 207 (2013); Ohio Informal Ethics Op. 2013-13 (2013); Penn. Formal Ethics Op. 2011-200 (undated).

Often, in house counsel has no input with regard to the technology used by the corporation, but owes the duty of communication with the corporate client regarding the risks and benefits of cloud storage. Comment 3 to RPC 1.13[2] states that when constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province.

Use of the technology is ethically proper if the lawyer abides by the Rules of Professional Conduct: to act competently, RPC 1.1[3], to take reasonable measures to protect the confidentiality, security, and accessibility of client information stored and transmitted through the cloud, RPC 1.6[4, 5, 6] and 1.9(c)[7]; by competently choosing the provider of the cloud services.

The lawyer is not required by the rules to use infallible methods of protection. "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..." RPC 1.6, cmt. [16]6. "...Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise affected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality." Me. Ethics Op. 207 (2013); N. C. 2011 Formal Ethics Op. 6 (2012). "Special circumstances, however, may warrant special precautions." RPC 1.6, cmt. [16]6. What safeguards are appropriate depends upon the nature and sensitivity of the data. Alaska Ethics Op. 2014-3 (2014).

Fla. Ethics Op. 12-3 (2012) states that lawyers should "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."

The duties of competence 3 and confidentiality 4, 5, 6 owed to the client by the lawyer are ongoing and are not delegable.[8, 9, 10] While competence does not require a lawyer to become an expert in data storage, it does require that the lawyer remain aware of how and where data are stored and what the provider service agreement says. Alaska Ethics Op. 2014-3 (2014).

The American Bar Association Model Rule of Professional Conduct 1.1,[11] which is identical in its wording to Rule 1.1 of the Tennessee Rules of Professional Conduct, has amended its Model Rule Comment on maintaining competence to include keeping abreast of changes "including the benefits and risks associated with relevant technology". Otherwise the comment is the same as the Tennessee version of the comment on maintaining competence.

Because the delegation of file storage to a provider of cloud computing services adds a layer between the lawyer and confidential client information over which the lawyer has responsibility, competence also requires that the lawyer ensure that tasks are delegated to competent service providers which the lawyer has selected after investigating the qualifications, competence, and diligence of the provider to ensure that client information is reasonably likely to remain confidential and secure through storage and retrieval. Ky. Ethics Op. E-437 (2014). The primary obligation is to select a reliable provider under the circumstances. In making this selection, the lawyer should consider the provider's ability to protect the information, to limit authorized access only to necessary personnel and to ensure that the information is backed up, is reasonably available to the lawyer and is reasonably safe from unauthorized intrusion. Alaska Ethics Op. 2014-3 (2014); Penn. Formal Ethics Op. 2011-200 (undated).

Suggested guidelines in helping lawyers competently choose the provider of the cloud services with the Rules of Professional Conduct are set forth in the following opinions:[12]

Ala. Ethics Op. 2010-02 (2010) concludes "that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so." The Commission defined "reasonable care" as requiring the lawyer to:

1. Learn how the provider would handle the storage and security of the data;

2. reasonably ensure that the provider abides by a confidentiality agreement in handling the data; and

3. stay abreast of appropriate safeguards that should be employed by both the lawyer and the third party.

N. C. 2011 Formal Ethics Op. 6 (2012) and Me. Ethics Op. 207 (2013) suggest that in dealing with providers of cloud computing services or hardware, lawyers should adopt additional safeguards made relevant by the Rules of Professional Conduct, such as:

1. An agreement between the cloud service provider and the lawyer or law firm that the provider will handle confidential client information in keeping with the lawyer's professional responsibilities.

2. If the lawyer terminates use of the cloud computing services or product, the provider goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code.

3. Careful review of the terms of the law firm's user or license agreements with the provider, including the security policy.

4. Evaluation of the cloud provider's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored

data.

Pa. Formal Ethics Op. 2011-200 (undated), Maine Ethics Op. 207 (2013), N.H. Advisory Ethics Op. 2012-13/4 (2013) and Ohio Informal Ethics Op. 2013-13 (2013) listed issues which lawyers should consider before using a cloud computing service, including that the service provider:

- will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
- has procedures to respond to government or judicial attempts to obtain disclosure of client data;

Lawyers also need to have internal policies and procedures to aid in complying with the Rules of Professional Conduct with regard to cloud computing. Penn. Formal Ethics Op. 2011-200 (undated) and Me. Ethics Op. 207 (2013) list internal policies and procedures that lawyers should adopt in connection with cloud usage such as:

1. backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;

2. educating and training employees of the firm who use cloud computing to abide by all end user security measures, including, but not limited to, the creation and regular replacement of passwords.

CONCLUSION

A lawyer may use cloud-based services with regard to confidential client information. In using cloud-based services, a lawyer must use reasonable care to assure that client confidentiality is protected and client property is safeguarded. See, RPC 1.6(a) and 1.9(c). A lawyer must comply with his or her duty of competence in the selection and continued use of the providers of cloud-based services. See, RPC 1.1. A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services is compatible with ethical obligations of the lawyer, and, if the lawyer is a partner or otherwise has managerial authority in a law firm, the lawyer must use "reasonable efforts" to make sure that the firm has measures in place to assure that providers of cloud-based services engage in conduct compatible with ethical obligations of the lawyer. See, RPC 5.3(a) & (b).

This 11th day of September, 2015.

ETHICS COMMITTEE:

Wade Davies
H. Scott Reams
Michael Callaway

APPROVED AND ADOPTED BY THE BOARD

[1] Ala. Ethics Op. 2010-02 (2010); Alaska Ethics Op. 2014-3 (2014); Ariz. Ethics Op. 09-04 (2009); Cal. Ethics Op. 2010-179 (2010); Conn. Informal Op. 2013-07 (2013); Fla. Ethics Op. 12-3 (2012); Iowa Ethics Op. 11-01 (2011); Ky. Ethics Op. E-437 (2014); Me. Ethics Op. 207 (2013); Mass. Ethics Op. 12-03 (2012); N.H. Adv. Ethics Op. 2012-13/4 (2013); N.Y. Ethics Op. 842 (2010); Nev. Ethics Op. 33 (2006); N. C. 2011 Formal Op. 6 (2012); Ohio Informal Ethics Op. 2013-13 (2013); Or. Ethics Op. 2011-188 (2011); Penn. Formal Ethics Op. 2011-200 (undated); Va. Legal Ethics Op. 1872 (2013); Wash. Advisory Op 2215 (2012).

[2] Comment [3], to RPC 1.13 provides:

When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonably necessary in the best interest of the organization. As defined in RPC 1.0(f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[3] RPC 1.1 Competence, provides:

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

[4] Rule 1.6 (a): Confidentiality of Information provides:

(a) A lawyer shall not reveal information relating to the representation of a client unless:

1. the client gives informed consent;

2. the disclosure is impliedly authorized in order to carry out the representation; or

3. the disclosure is permitted by paragraph (b) or required by paragraph (c).

[5] Comment [15], Acting Competently to Preserve Confidentiality, to RPC 1.6 provides:

[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 RPCs 1.1, 5.1, and 5.3.

[6] Comment [16], to RPC 1.6 provides:

[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.

[7] Rule 1.9: Duties to Former Clients, provides in part:

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter reveal information relating to the representation or use such information to the disadvantage of the former client unless (1) the former client gives informed consent, confirmed in writing, or (2) these Rules would permit or require the lawyer to do so with respect to a client, or (3) the information has become generally known.

[8] Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers, provides in part:

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

[9] Rule 5.3: Responsibilities Regarding Nonlawyer Assistants, provides:

With respect to a nonlawyer employed, 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 nonlawyer's conduct is compatible with these Rules;

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

[10] Comment [1] to RPC 5.3 provides:

[1] Lawyers generally employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyer assistants should take account of the fact that they do not have legal training and are not subject to professional discipline.

11

Maintaining Competence [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. Underlining added.

[12] The Board is not adopting these opinions, but they are set forth as guidance to consider.

Mission Statement

To assist the Court in protecting the public from harm from unethical lawyers by administering the disciplinary process; to assist the public by providing information about the judicial system and the disciplinary system for lawyers; and, to assist lawyers by interpreting and applying the Court's disciplinary rules.

(/)

1. Client-Lawyer Relationship

Related Opinions (/Ethics/EthicsOpinions/RelatedOpinions?id=26)

ER 1.6. Confidentiality of Information

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

(b) A lawyer shall reveal such information to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal act that the lawyer believes is likely to result in death or substantial bodily harm.

(c) A lawyer may reveal the intention of the lawyer's client to commit a crime and the information necessary to prevent the crime.

(d) A lawyer may reveal such 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 fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(2) to 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 compliance with 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 final order of a court or tribunal of competent jurisdiction directing the lawyer to disclose such information.

(6) to prevent reasonably certain death or substantial bodily harm.

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(e) 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.

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 ER 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, ER 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 ERs 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 ER 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The public is better protected if full and open communication by the client is encouraged than if it is inhibited. 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 also applies in such situations 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.

[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 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.

[6] The requirement of maintaining confidentiality of information relating to representation applies to government lawyers who may disagree with the policy goals that their representation is designed to advance.

Disclosure Adverse to Client

[7] 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. Paragraph (b) recognizes the overriding value of life and physical integrity, and requires the lawyer to make a disclosure in order to prevent homicide or serious bodily injury that the lawyer reasonably believes is intended by a client. In addition, under paragraph (c), the lawyer has discretion to make a disclosure of the client's intention to commit a crime and the information necessary to prevent it. It is very difficult for a lawyer to "know" when such unlawful purposes will actually be carried out, for the client may have a change of mind.

[8] Paragraph (c) permits the lawyer to reveal the intention of the lawyer's client to commit a crime and the information necessary to prevent the crime. Paragraph (c) does not require the lawyer to reveal the intention of a client to commit wrongful conduct, but the lawyer may not counsel or assist a client in conduct the lawyer knows is criminal or fraudulent. See ER 1.2(d); see also ER 1.16 with respect to the lawyer's obligation or right to withdraw from the representation from the client in such circumstances. 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 ER 1.13(b).

[9] The range of situations where disclosure is permitted by paragraph (d)(1) of the Rule is both broader and narrower than those encompassed by paragraph (c). Paragraph (c) permits disclosure only of a client's intent to commit a future crime, but is not limited to instances where the client seeks to use the lawyer's services in doing so. Paragraph (d)(1), on the other hand, applies to both crimes and frauds on the part of the client, and applies to both on-going conduct as well as that contemplated for the future. The instances in which paragraph (d)(1) would permit disclosure, however, are limited to those where the lawyer's services are or were involved, and where the resulting injury is to the financial interests or property of others. In addition to this Rule, a lawyer has a duty under ER 3.3 not to use false evidence.

[10] Paragraph (d)(2) addresses the situation in which the lawyer does not learn of the client's crime or fraud until after it has been consummated. Although the client no longer has the option of preventing disclosure by refraining from the wrongful conduct, there will be situations in which the loss suffered by the affected person can be rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to mitigate reasonably certain losses or to attempt to recoup their losses. Paragraph (d)(2) does not apply when a person who has committed a crime or fraud thereafter employs a lawyer for representation concerning that offense.

[11] 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 (d)(3) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

[12] 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 (d)(4) 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.

[13] A lawyer entitled to a fee is permitted by paragraph (d)(4) to prove the services rendered in an action to collect it. 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.

[14] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes ER 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 ER 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (d)(5) permits the lawyer to make such disclosures as are necessary to comply with the law.

[15] Paragraph (d)(5) also permits compliance with a court order requiring a lawyer to disclose information relating to a client's representation. If a lawyer is called as a witness to give testimony concerning a client or is otherwise ordered to reveal information relating to the client's representation, however, the lawyer must, absent informed consent of the client to do otherwise and except for permissive disclosure under paragraphs (c) or (d), assert on behalf of the client all nonfrivolous claims that the information sought is protected against disclosure by this Rule, the attorney-client privilege, the work product doctrine, or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal. See ER 1.4. Unless review is sought, however, paragraph (d)(5) permits the lawyer to comply with the court's order.

[16] In situations not covered by the mandatory disclosure requirements of paragraph (b), paragraph (d)(6) permits discretionary disclosure when the lawyer reasonably believes disclosure is necessary to prevent reasonably certain death or substantial bodily harm.

[17] Paragraph (d)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See ER 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only when there is a reasonable possibility that a new relationship might be established. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these ERs.

[18] Any information disclosed pursuant to paragraph (d)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (d)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (d)(7). Paragraph (d)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[19] Paragraph (d) 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.

[20] Paragrach (d) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (d)(1) through (d)(5). 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 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 (d) 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 this Rule. See ERs1.2(d), 4.1(b), 8.1 and 8.3. ER 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See ER 3.3(b).

Withdrawal

[21] 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 ER 1.16(a)(1). After withdrawal the lawyer is required to refrain from making disclosure of the client's confidences, except as otherwise provided in ER 1.6. Neither this Rule nor ER 1.8(b) nor ER 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.

Acting Competently to Preserve Confidentiality

[22] Paragraph (e) 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 ERs 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 (e) 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 ER or may give informed consent to forgo security measures that would otherwise be required by this ER. 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 ERs. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see ER 5.3, Comments [3]–[4].

[23] 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 ER or may give informed consent to the use of a means of communication that would otherwise be prohibited by this ER. 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 ERs.

Former Client

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

CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW℠

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

A CNA PROFESSIONAL COUNSEL GUIDE FOR LAWYERS AND LAW FIRMS

CLOUD COMPUTING – AN OVERVIEW

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

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

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

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

THE POTENTIAL BENEFITS OF CLOUD COMPUTING FOR LAW PRACTICE MANAGEMENT

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

1. Reduced Cost/Reduced Capital Expenditures

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

2. Scalability/Flexibility

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

3. Accessibility of Data Across Different Devices

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

4. Sharing/Collaboration

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

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

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

ETHICAL IMPLICATIONS OF USING THE CLOUD IN LAW PRACTICE

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

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

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

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

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

RISKS OF MOVING TO A CLOUD STORAGE SYSTEM

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

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

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

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

Appendix A

NON-EXCLUSIVE LIST OF CLOUD VENDORS[11]

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

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

Appendix B

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

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

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

I. PHYSICAL SECURITY

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

II. OWNERSHIP OF DATA

Example 1

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

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

Example 2

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

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

III. DUTY IN EVENT OF BREACH

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

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

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

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

IV. STORAGE LOCATION, VENUE AND CHOICE OF LAW

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

V. CONFIDENTIALITY

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

VI. AUDIT OF VENDOR

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

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

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

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

Appendix C

DRAFT LETTER ADVISING CLIENT OF USE OF CLOUD STORAGE

Client Important
Address
Re: Notice of Use of Cloud Storage

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

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

Very truly yours,

Ms. Attorney

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

Appendix D

CLOUD VENDOR CHECKLIST

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

continued on next page

CLOUD VENDOR CHECKLIST *(continued)*

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

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

State Bar of Arizona Ethics Opinions

07-02: Maintaining Client Files; Client's Papers and Documents; Electronic Storage

6/2007

In appropriate cases, a lawyer may keep current and closed client files as electronic images in an attempt to maintain a paperless law practice or to more economically store files.

After digitizing paper documents, a lawyer may not, without client consent, destroy *original* paper documents that belong to or were obtained from the client. After digitizing paper documents, a lawyer may destroy *copies* of paper documents that were obtained from the client unless the lawyer has reason to know that the client wants the lawyer to retain them. A lawyer has the discretion to decide whether to maintain the balance of the file solely as electronic images and destroy the paper documents.

FACTS

Many lawyers have requested informal ethics advice about whether they may maintain current and certain closed client files as electronic images instead of as paper documents. Some have indicated they want to digitize closed client files (and then destroy the paper file) because of the increasing cost of storing files. Others have indicated that they wish to maintain only electronic images of current client files, both to save storage space and because they believe electronic images are easier to manage and organize. In both circumstances, these lawyers have inquired about their ability to maintain only digitized files and destroy the paper copies, and their associated obligations to their clients. In light of these frequent requests for informal ethics advice, the Committee on the Rules of Professional Conduct has chosen to issue this formal opinion *sua sponte*.

QUESTIONS PRESENTED

Lawyers have asked for ethics advice on variations on the following questions:

1. May a lawyer keep *current* client files only as electronic images, and then destroy the converted paper documents, in an attempt to maintain a paperless law practice?

2. May a lawyer digitize client files that are *closed* – but not yet eligible for total destruction – and then destroy the paper documents?

RELEVANT ETHICAL RULES

ER 1.15 Safekeeping Property

> (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, or elsewhere with the consent of the client or third person. 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 five years after termination of the representation.
>
> . . . .

ER 1.16 Declining or Terminating Representation

> . . .
>
> (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 documents and property to which the client is entitled and refunding any advance payment of a fee that has not been earned. Upon the client's request, the lawyer shall provide the client with all of the client's documents, and all documents reflecting work performed for the client. The lawyer may retain documents reflecting work performed for the client to the extent permitted by other law only if retaining them would not prejudice the client's rights.

RELEVANT ARIZONA ETHICS OPINIONS

Ariz. Ethics Ops. 98-07 (http://www.myazbar.org/Ethics/opinionview.cfm?id=492), 05-04 (http://www.myazbar.org/Ethics/opinionview.cfm?id=523)

OTHER ETHICS OPINIONS

Virginia Legal Ethics Op. 1818 (2005)

OPINION

This opinion does not involve the typical issues of file retention, in which a lawyer seeks to destroy and not retain closed client files. Rather, this opinion addresses a lawyer's desire to maintain active client files or retain closed files solely as electronic images instead of paper documents and then to destroy the paper documents.

Ariz. Ethics Op. 05-04 concluded that it is not unethical to store client information and confidences on computer systems. This opinion takes Op. 05-04 one step further by addressing whether a lawyer may, to use the vernacular, go paperless, keeping the entire file solely in electronic form by digitizing all documents.

At issue is converting file documents to electronic images, such as to Adobe's well-known portable document format (pdf), not simply storing word-processing documents or email messages or, in fact, saving electronic image files or databases received from the client or third parties.

This practice implicates traditional file-retention issues because although scanning a paper document into a computer and storing the resulting data as a digital image may result in a duplicate image of the paper document, that image exists nonetheless in a medium different than the paper document. To achieve the goal of going paperless, a lawyer would need to destroy the paper document, thus raising the issue of which paper documents the lawyer controls and may opt to destroy.

Ariz. Ethics Op. 98-07, our seminal opinion on file retention following termination of representation, provides the starting point for analyzing this issue. That opinion reached several relevant conclusions:

- The client generally owns materials in a client's file the lawyer obtained from the client.

- At the end of representation, a lawyer is ethically required to use reasonable efforts to return all client property, including materials in a client's file, to the client.

- If the lawyer is unable to return the materials to the client, the lawyer then may consider the material abandoned and, after waiting for the five-year holding period dictated by the Uniform Unclaimed Property Act, *in some cases* may destroy the file.

- The balance of the file generally belongs to the lawyer, but the former client has an interest in and right to access the file.

Op. 98-07 at 9-10.

Although that opinion dealt with file retention following the termination of representation, the conclusions listed above also apply in advising lawyers whether they may maintain active or closed files solely as digital images and whether they may then destroy the digitized paper files.[1]

Op. 98-07 differentiated between documents provided to the lawyer by the client and the balance of the file. The same differentiation applies in answering the questions posed in this opinion.

1. Authority to decide whether to store the file solely as a digital image

a. Documents obtained from the client

A literal reading of Op. 98-07's statement that "[m]aterials in a client's file obtained from the client are generally owned by the client" would lead to the conclusion that after digitizing paper documents, a lawyer may not unilaterally decide to destroy any of the documents – whether originals or copies – that were obtained from the client.

In the context of digitizing documents in a client file, however, we see a dichotomy between originals and copies. Clearly, a lawyer may not digitize and then, without the client's consent, destroy original documents obtained from the client. The digitized version is not the same as the original, and the client has an interest

in maintaining the integrity of the original documents.

A photocopy, on the other hand, already is a substitute for the original. Rigidly applying Op. 98-07's statement to copies of documents obtained from a client would mean, for example, that in a document-laden case, the lawyer would have to obtain the client's consent to discard – after digitizing – every photocopy or facsimile the client transmitted to the lawyer.

A less rigid approach is more realistic in this situation. The lawyer is not, after all, destroying the information. Instead, the lawyer is keeping the image of the document – already imaged by the photocopy – in a different format. We therefore conclude that after digitizing a photocopy or facsimile of a document, the lawyer may destroy the hard copy *unless the lawyer has reason to know that the client does not or would not want the lawyer to discard it*. For example, if a photocopy is the only available version of an original, digitizing and then destroying the photocopy may not be prudent. On the other hand, if a client has supplied the lawyer with a photocopy of a document and has kept the original, either on his or her own initiative or at the lawyer's direction, the lawyer may have no reason to know that the client expects the lawyer to keep the photocopy as a paper document.

The lawyer of course may avoid any questions by obtaining the client's consent at the beginning of representation, during representation when the client provides documents to the lawyer, or at a later time, such as at the conclusion of representation. For example, if the client provides the lawyer with photocopies of documents, the lawyer could clarify with the client that the documents are for the lawyer's use and may be destroyed after the lawyer digitizes them.

Alternatively, the lawyer may avoid any questions by, after digitizing the documents, returning them to the client.

One specific category of records – letters from clients – does not fall neatly within the dichotomy described above. Technically, under Op. 98-07 and our analysis in this opinion, a letter from a client to a lawyer would be an original document obtained from a client. On the other hand, that letter from a client may convey photocopies of documents for the lawyer's own use. It would be illogical to advise that the lawyer could digitize and then destroy those photocopies but not the cover letter from the client conveying them. We conclude, therefore, that letters from clients do not fall into the category of "[m]aterials in a client's file obtained from the client" but instead are part of the "balance of the file" over which the lawyer has unilateral authority and discretion.

b. Balance of the file

In general, we see nothing *per se* unethical with a lawyer choosing to maintain the balance of a file, whether active or closed, solely as electronic images. Neither ER 1.15 nor ER 1.16 dictates that a lawyer must keep a client's legal file in paper form. *See* Virginia Legal Ethics Op. 1818 (2005). We agree with the Virginia opinion that

> [i]n determining whether an attorney is meeting his ethical responsibilities for a particular client, it matters not generally what form the documents in the file take, but instead whether all the documents necessary for the representation are present in the file.

In addition, Op. 98-07 concluded that although the client owns file materials the lawyer has obtained from the client, "[t]he balance of the file generally belongs to the lawyer." *Id.* at 10. This has been a somewhat confusing statement to apply in light of a lawyer's obligations under ER 1.16 and even within the context of Op. 98-07 itself.[2] Nonetheless, the important concept for this opinion is the scope of the lawyer's authority over the file other than documents obtained from the client. Whatever else "generally belongs to the lawyer" may mean, it at the very least means that the lawyer has the authority to decide whether to keep "[t]he balance of the file" as paper or as digital images.

2. Discretion to decide whether to store the file solely as a digital image

As in any case, a lawyer contemplating maintaining a client's file solely in electronic form will need to determine if it is in the client's best interest to do so. Many cases may involve legally operative documents that should be maintained in their original form. On the other hand, a photocopy of a document may be just as valuable for evidentiary purposes as the original, and a digital image of the photocopy may degrade that value.

In deciding whether to maintain client files solely as electronic images, a lawyer also must keep in mind the lawyer's obligation to provide the client access to the file. At termination of representation, the lawyer is obligated to "take steps to the extent reasonably practicable to protect a client's interests, such as... surrendering documents and property to which the client is entitled...." ER 1.16(d). In addition, "[u]pon the client's request, the lawyer shall provide the client with all of the client's documents, and all documents reflecting work performed for the client." *Id.* We interpret this as requiring the lawyer to provide meaningful access. A lawyer who has chosen to store his or her client files digitally cannot simply hand a disk or other storage medium to a client without confirming that the client is able to read the digitized images. If the client does not have either the technological knowledge or access to a computer on which to display the electronic images, or if the client has hired substitute counsel who is in the same position as the client, the original lawyer may need to provide paper copies of the documents. If the lawyer has opted to store the file solely as digital images for his or her own convenience, the lawyer will need to bear the cost of providing those paper copies, absent other agreed-upon arrangements.[3]

Although the lawyer must provide the client with meaningful access to the file, we do not believe the lawyer must obtain the client's consent to maintain solely as electronic images documents other than those provided by the client and with the considerations described above.[4] Nonetheless, the lawyer must maintain the electronic images in such a manner as will permit them to be readily and accurately convertible into paper format within a reasonable period of time.

In addition, if a lawyer wishes to store client files solely as electronic images and not keep paper copies, the lawyer must take reasonable steps to ensure that the digitized file is complete. Just as photocopiers and printers may skip pages, so may scanners, and if the lawyer has destroyed the paper document, then the file will be incomplete. Naturally, when converting a document to a digital image, the lawyer also must take reasonable precautions to avoid damaging the documents. With rare or difficult-to-replace documents, it should not be attempted.

Finally, a lawyer who wishes to maintain the allowable portions of a client file solely as electronic images must consider whether the format lends itself to long-term storage. Until the time a file may legitimately be destroyed, a lawyer who maintains that file solely as digitized images will need to use technology that

permits the file to be readily and accurately retrievable. In addition, the lawyer should be familiar with or take steps to insure that the digital-storage medium is properly stored to maintain its shelf life.

CONCLUSION

In appropriate cases and with appropriate safeguards, a lawyer ethically may keep active and closed client files as electronic images in an attempt to maintain a paperless law practice, with the understanding that he or she may need to provide paper versions to the client and any subsequent attorney. However, until the file legitimately may be destroyed, as detailed by Op. 98-07, a lawyer may not, without client consent, destroy original paper documents that belong to or were obtained from the client. Similarly, a lawyer may not, without client consent, convert to digital images and then destroy photocopies or facsimiles of documents obtained from the client if the lawyer has reason to know the client expects the lawyer to keep the paper documents.

---

[1] This opinion only addresses a lawyer's ethical duties to maintain client files, not whether digitized documents would be valid under particular statutes or administrative or court rules. In addition, as we noted in Op. 98-07, file retention and destruction policy often is a subject of court rule or statute. We do not offer an opinion as to any legal requirements for document retention or destruction or the legal ownership of all or any portions of client files.

[2] The relevant comments to ER 1.16 state:

> [9] Ordinarily, the documents to which the client is entitled, at the close of the representation, include (without limitation) pleadings, legal documents, evidence, discovery, legal research, work product, transcripts, correspondence, drafts, and notes, but not internal practice management memoranda. A lawyer shall not charge a client for the cost of copying any documents unless the client already has received one copy of them.
>
> . . .
>
> [11] Lawyers may fulfill their ethical obligations with respect to client files by returning the file to the client. File retention policies should be disclosed to the client, preferably in writing and at the inception of the relationship.
>
> [Emphasis added.] While stating that the file generally "belongs to" the lawyer, except for documents obtained from the client, Op. 98-07 nonetheless acknowledged that the lawyer "may fulfill her ethical obligations by tendering the entire file to the client...at termination of representation." Op. 98-07 at 10. It is inconsistent to advise that the file "belongs to" the lawyer yet also warn that the lawyer may need to tender or return it to the client at the conclusion of the representation.

[3] This does not mean, however, that the lawyer must bear the cost of converting the images to a client's, or a successor lawyer's, preferred format. The lawyer and client and/or successor counsel could negotiate this issue.

[4] Virginia Op. 1818 advised that the lawyer must obtain client consent before destroying the paper documents. That opinion does not distinguish between documents provided by the client and other documents – the distinction we made in Op. 98-07 – even though the opinion noted that the lawyer is in the "better position to know in what circumstances there may be legal significance in keeping the paper versus the electronic version of file contents...." With the caveat that a lawyer must determine if it is in the client's best interest to keep only a digitized version of documents, we do not believe that the lawyer must obtain client consent before doing so, provided, of course, that the lawyer ensures that the client has meaningful access to the file.

State Bar of Arizona Ethics Opinions

07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure 11/2007

While modern electronic communications are often greatly beneficial to the client, lawyers who use them to send or receive documents or other communications on behalf of clients must be aware that they carry certain risks. Lawyers must take reasonable precautions to prevent inadvertent disclosure of confidential information.

Except in the specific circumstances described in this opinion, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it.

FACTS

This opinion addresses the ethical duties of lawyers who send and receive electronic communications. Such communications may contain metadata. Metadata is information describing the document's history, tracking, and management. Metadata may also include hidden information, such as track changes, comments, and other information. By "mining" the metadata in a document, it may be possible to identify the author of the document, the changes made to the document during the various stages of its preparation and revision, comments made by the persons who prepared or reviewed the document, and other documents embedded within the document.

For example, a lawyer who is preparing a document may electronically circulate the document in draft form among other lawyers in the firm for their review and comment. The other lawyers may insert their suggested revisions and other comments, some of which might address the strengths and weaknesses of the client's position. If the final version of the document is electronically transmitted to opposing counsel, it may be possible for opposing counsel to discover the comments.

The sender of the document may not be aware of the metadata embedded within the document or that it remains in the electronic document despite the sender's good faith belief that it was "deleted." In most cases, metadata is inconsequential or otherwise known to the recipient of the document. In some situations, though, the metadata in the electronic document may permit the recipient of the document to obtain information that is confidential or privileged from disclosure. Given the importance of this subject matter, the Committee has determined that it is appropriate to issue a *sua sponte* opinion for the guidance of lawyers in Arizona.

QUESTIONS PRESENTED

1. If a lawyer sends an electronic communication, what ethical duty does the lawyer have to prevent the disclosure, through metadata embedded therein, of confidential or privileged information?

2. May a lawyer who receives an electronic communication examine it for the purpose of discovering the contents of the metadata that may be embedded within it?

RELEVANT ETHICAL RULES

ER 1.6 Confidentiality of Information

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

ER 4.4 Respect for Rights of Others

> . . .
>
> (b) A lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures.

ER 8.4 Misconduct

> It is professional misconduct for a lawyer to:
>
> (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;
>
> (b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;
>
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
>
> (d) engage in conduct that is prejudicial to the administration of justice;
>
> . . . .

RELEVANT ETHICS OPINIONS

ABA Formal Op. 06-442; Ala. Op. RO-2007-02; D.C. Op. 341; Fla. Op. 06-2; N.Y. State Bar Ops. 749 and 782

OPINION

Duties of the Sender

"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." ER 1.6, cmt 20. What is "reasonable" in the circumstances depends on the sensitivity of the information, the potential consequences of its inadvertent disclosure, whether further disclosure is restricted by statute, protective order, or confidentiality agreement, and any special instructions given by the client. *Id*. *See also* Ala. Op. RO-2007-02 (March 14, 2007); Fla. Op. 06-2 (September 15, 2006); N.Y. State Bar Op. 782 (December 8, 2004). In the case of a lawyer who is employed by a corporation or by a governmental or other entity, "special instructions given by the client" might include the client's informed consent to forego, for financial or other reasons, the acquisition or use of software that is designed to remove metadata from an electronic document. If a lawyer is asked to comment on a document prepared by another lawyer in the firm, and the commenting lawyer knows or reasonably should know that the document is ultimately intended for transmission to opposing counsel, he or she should consider whether the comment is the type that should be included within the draft. A lawyer who prepares a pleading, contract, or other document should use a "clean" form and not a document that was used for another client. The lawyer who sends an electronic document should be aware that the electronic document may be received or distributed to a person who is not a lawyer and who therefore does not have the duties of a recipient lawyer with respect to such document.

When removing or restricting access to metadata in documents produced or disclosed in litigation, the lawyer must take care not to violate any duty of disclosure to which the lawyer or the lawyer's client is subject. For a recent discussion relating to the duty to preserve and disclose metadata in a litigation context, see *Wyeth v. Impax Laboratories, Inc.*, 2006 WL 3091331 (D. Del. October 26, 2006). *See also* the Arizona Supreme Court's order dated September 5, 2007, on rule-change petition R-06-0034 (amending, effective January 1, 2008, the Arizona Rules of Civil Procedure to include provisions relating to discovery and disclosure of "electronically stored information").

Duties of the Recipient

> A fundamental principle of 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.... This contributes to the trust that is the hallmark of the client-lawyer relationship. The public is better protected if full and open communication by the client is encouraged than if it is inhibited. 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.

ER 1.6, cmt 2 (internal citations omitted).

Lawyers, in light of this fundamental principle, and in keeping with their status as members of a learned profession, should refrain from conduct that amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel. ER 8.4(a)-(d). *See also* Ala. Op.

RO-2007-02.

Florida, in Op. 06-2, concluded that "[a] lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer." The New York State Bar Association, in Op. 749 (December 14, 2001), determined that a lawyer may not "intentional[ly] use . . . computer technology to surreptitiously obtain privileged or other confidential information" of an opposing party. Alabama, in Op. RO-2007-02, has adopted the New York position.

The American Bar Association (ABA), in Formal Op. 06-442 (August 5, 2006), concluded that the Model Rules of Professional Conduct do not prohibit such conduct. We respectfully decline to follow the ABA position. Despite the most reasonable and thorough precautions, and even with the best of intentions, it may not be possible for the sending lawyer to be absolutely certain that all of the potentially harmful metadata has been "scrubbed" from the document before it is transmitted electronically. Under the ABA position, the sending lawyer would be at the mercy of the recipient lawyer. Under such circumstances, the sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely. We do not think that is realistic or necessary. Under the position adopted by Florida, New York, Alabama, and now Arizona, the sending lawyer is alerted to the potential problem and is reminded of the duty to take reasonable steps to prevent the inadvertent disclosure of confidential or privileged information. At the same time, except in the specific circumstances described below, the recipient lawyer has a corresponding duty not to "mine" the document for metadata that may be embedded therein or otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel.[1]

We also note that there is a significant difference between the Model Rules of Professional Conduct as promulgated by the ABA and the Rules of Professional Conduct as adopted by the Arizona Supreme Court. Under Arizona's version of ER 4.4(b), a "lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures." While it might be argued that ER 4.4(b) is inapplicable because the *document* was not inadvertently sent, only the metadata embedded therein, we think that is an insubstantial distinction. If the document as sent contains metadata that reveals confidential or privileged information, it was not sent in the form in which it was intended to be sent, and the harm intended to be remedied by ER 4.4(b) is the same. Therefore, a lawyer who receives an electronic document from another party, and who discovers metadata embedded in the document that the lawyer knows or reasonably should know is revealing confidential or privileged information, has a duty to notify the sender and to preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures. ER 4.4(b). We express no opinion on whether any evidentiary privilege continues to exist once an inadvertent disclosure has occurred, or whether the lawyer has incurred civil liability as the result of such disclosure. Those are questions of substantive law. Whether the sending lawyer has transgressed ER 1.6 will depend on what was reasonable in the circumstances.

We recognize that some metadata embedded within an electronic document may be discovered by the recipient through inadvertent or relatively innocent means, such as right-clicking a mouse or by holding the cursor over certain text in the document. We do not mean to imply that all such activity necessarily rises to a level of ethical concern. If, however, the recipient discovers metadata by any means, and knows or reasonably should know that the sender did not intend to transmit the information, the recipient has a duty to follow the procedures set forth in ER 4.4(b).

A lawyer who receives an electronic communication may attempt to discover the metadata that is embedded therein if he or she has the consent of the sender, or if such conduct is allowed by a rule, order, or procedure of a court or other applicable provision of law. Even so, if the lawyer comes across information that the lawyer knows or reasonably should know was not intended to be transmitted by the sender, the recipient has a duty to follow the procedures set forth in ER 4.4(b).

CONCLUSION

Lawyers who send communications or other documents electronically must be aware that such activity has inherent risks. Therefore, the lawyer must take reasonable measures to prevent the inadvertent disclosure of confidential client information. At the same time, and except in the specific circumstances set forth above, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it. A recipient lawyer who discovers metadata embedded within an electronic communication and who knows or reasonably should know that the metadata reveals confidential or privileged information has a duty to comply with the procedures set forth in ER 4.4(b).

---

[1] The District of Columbia, in Op. 341 (September 2007), held that "[a] receiving lawyer is prohibited from reviewing metadata sent by an adversary *only* where he has actual knowledge that the metadata was inadvertently sent." (Emphasis added). While Op. 341 may reflect an effort to reach a middle ground between the position of the ABA, on the one hand, and the positions of Alabama, Florida, and New York on the other hand, we respectfully disagree with the District of Columbia. Subject to the specific exceptions described elsewhere in this opinion, a lawyer who receives an electronic communication should not be engaged in the intentional examination of the document's metadata in the first place and, in our view, would bear the burden of establishing that any such intentional examination was for a proper purpose and not for the purpose of attempting to discover any confidential or privileged information that might be contained therein.

(/)

Member Login Search

State Bar of Arizona Ethics Opinions

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

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

FACTS

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

QUESTION PRESENTED

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

APPLICABLE ARIZONA RULES OF PROFESSIONAL CONDUCT ("ER __")

ER 1.1 Competence

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

ER 1.6 Confidentiality of Information

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

RELEVANT ARIZONA ETHICS OPINIONS

Ariz. Ethics Ops. 05-04 (http://www.myazbar.org/Ethics/opinionview.cfm?id=523), 07-02 (http://www.myazbar.org/Ethics/opinionview.cfm?id=694)

OPINION

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

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

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

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

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

It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field. The competence requirements of ER 1.1 apply not only to a lawyer's legal skills, but

also generally to "those matters reasonably necessary for the representation." Therefore, as a necessary prerequisite to making a determination regarding the reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security.

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

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

CONCLUSION

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

---

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

(/)

Member Login Search

1. Client-Lawyer Relationship

Related Opinions (/Ethics/EthicsOpinions/RelatedOpinions?id=3)

ER 1.1. Competence

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

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 impracticable. 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 ER 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 ER 1.2(c).

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.

[7] A lawyer, whether appointed or retained, who represents a defendant in a capital case shall comply with the standards for appointment of counsel in capital cases set forth in the Arizona Rules of Criminal Procedure.