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

**Amended September 8, 2017**[1]

## Synopsis

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

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

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

## Introduction

Technology has dramatically changed the practice of law in many ways, including the ways in which lawyers process, transmit, store, and access client information. Perhaps no area has seen greater change than "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your

[1] This opinion was amended to reflect changes in Wisconsin's Rules of Professional Conduct for Attorneys.

computer."[2] In other words, cloud computing includes the processing, transmission, and storage of the client's information using shared computer facilities or remote servers owned or leased by a third-party service provider.[3] These facilities and services are accessed over the Internet by the lawyer's networked devices such as computers, tablets, and smart phones.[4]

Many lawyers welcome cloud computing as a way to reduce costs, improve efficiency, and provide better client service.[5] The cloud service provider assumes responsibility for infrastructure, application software, development platforms, developer and programming staff, licensing, updates, security and maintenance, while the lawyer enjoys access to the client information from any location that has Internet access. Along with the lawyer's increased accessibility comes the loss of direct control over the client's information. The provider of cloud computing adds a layer of risk between the lawyer and client's information because most of the physical, technical, and administrative safeguards are managed by the cloud service provider. Yet the ultimate responsibility for insuring the confidentiality and security of the client's information lies with the lawyer.

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

Ethics opinions from other states that have addressed the issue of cloud computing have generally concluded that a lawyer may use cloud computing if the lawyer makes reasonable efforts to adequately address the risks in doing so.[6] But the definition of what is reasonable varies.

---

[2] Pennsylvania Bar Ass'n Comm. On Legal Ethics and Professional Responsibility Formal Ethics Opinion 2011-200: Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property at 1 (2011)(quoting Quinn Norton, "Byte Rights," *Maximum PC,* September 2010, at 12). A more detailed definition is difficult to formulate because cloud computing is not a single system, but includes different technologies, configurations, service models, and deployment models. For example, cloud computing encompasses web-based email, online data storage, software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). Deployment models include public clouds, private clouds, hybrid clouds, and managed clouds.

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

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

[5] Many lawyers also welcome cloud technology as a way to operate a virtual law office. Recent ethics opinions, such as Ohio Board of Professional Conduct Opinion 2017-5 (June 2017), conclude that lawyers may practice law through a virtual law office, but must competently manage the technology used to run the practice.

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

The State Bar's Standing Committee on Professional Ethics (the "Committee") agrees with the conclusion of ethics opinions from other states that cloud computing is permissible as long as the lawyer makes reasonable efforts to adequately address the potential risks associated with it. Part I of this opinion identifies the specific rules of Wisconsin's Rules of Professional Conduct for Attorneys that are implicated by cloud computing and the duties imposed by those rules. Part II of this opinion discusses what constitutes reasonable efforts to protect the lawyer's access to and the confidentiality of client information.

## Part I: The Applicable Rules

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

### A. SCR 20:1.1 Competence

SCR 20:1.1 requires a lawyer to perform legal services competently.[7] ABA Comment [8], which follows SCR 20:1.1, recognizes that technology is an integral part of contemporary law practice and explicitly reminds lawyers that the duty to remain competent includes keeping up with technology.

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Moreover, ABA Comment [5], which follows SCR 20:1.1, recognizes that competency also requires the "use of methods and procedures meeting the standards of competent practitioners."

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

### B. SCR 20:1.4 Communication

SCR 20:1.4(b) requires that a lawyer explain a matter to the extent reasonably necessary to permit the client to make informed decisions concerning the representation.[8] While it is not necessary for a

---

[7] SCR 20:1.1 Competence

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

[8] SCR 20:1.4 Communication

(a) A lawyer shall:

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

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

lawyer to communicate every detail of a client's representation, the client should have sufficient information to participate intelligently in decisions concerning the objectives of representation and the means by which they are to be pursued.[9] Of concern is whether a lawyer must inform the client of the means by which the lawyer processes, transmits, and stores the client's information in all representations or only when the circumstances call for it, such as where the information is particularly sensitive.

None of the ethics opinions have suggested that a lawyer is required in all representations to inform the client of the means by which the lawyer processes, transmits, and stores information. One ethics opinion, however, suggests that a lawyer should consider giving notice to the client about the proposed method for storing client information.[10] Yet, lawyers' remote storage of client information is not a new occurrence: lawyers have been using off-site brick-and-mortar storage facilities for many years. Another opinion suggests that "it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of 'cloud computing' and the advantages as well as the risks endemic to online storage and transmission."[11]

While none of the ethics opinions have suggested that a client's informed consent is required in all instances before a lawyer may use cloud computing, one opinion has suggested that client consent may be necessary to use a third-party service provider when the information is highly sensitive.[12] If consent is required, SCR 20:1.4(a)(1) requires that the lawyer promptly inform the client.

The Committee agrees with other ethics opinions that a lawyer is not required in all representations to inform the client that the lawyer uses the cloud to process, transmit or store information. SCR 20:1.4 does not require the lawyer to inform the client of every detail of representation. It does, however, require the lawyer to provide the client with sufficient information so that the client is able to meaningfully participate in his or her representation. "The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation."[13]

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

---

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

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

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

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

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

[10] Vt. Ethics Op. 2010-6 (2011).

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

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

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

If there has been a breach of the provider's security that affects the confidentiality or security of the client's information, SCR 20:1.4(a)(3) and SCR 20:1.4(b) require the lawyer to inform the client of the breach.[14]

**C. SCR 20:1.6 Confidentiality**

The duty to protect information relating to the representation of the client is one of the most significant obligations imposed on the lawyer. SCR 20:1.6(a) prohibits a lawyer from revealing information relating to the representation of a client unless that client gives informed consent or unless the disclosure is impliedly authorized in order to carry out the representation.[15] The processing, transmission, and storage of information in the cloud may be deemed an impliedly authorized disclosure to the provider as long as the lawyer takes reasonable steps to ensure that the provider of the cloud computing services has adequate safeguards.[16]

SCR 20:1.6(d), which became effective January 1, 2017, requires that a lawyer "make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Although a lawyer has a professional duty to protect information relating to the representation of the client from unauthorized disclosure, this duty does not require any particular means of handling protected information and does not prohibit the employment of service providers who may handle documents or data containing protected information. Lawyers are not required to guarantee that a breach of confidentiality cannot occur when using a cloud service provider, and they are not required to use only infallibly secure methods of communication.[17] They are, however,

---

[14] While beyond the scope of this opinion, other law, such as Wis. Stat. § 134.98, may also require a lawyer to inform the client of a breach.

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

SCR 20:1.6 Confidentiality

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

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

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

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

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

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

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

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

(6) to detect and resolve conflicts of interest, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

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

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

required, to use reasonable efforts to protect information relating to the representation of their clients from unauthorized disclosure, regardless of the medium used.[18]

Moreover, ABA Comment [18], which follows SCR 20:1.6, emphasizes that unauthorized access to or the inadvertent or unauthorized disclosure of information relating to the representation of a client does not constitute a violation of the rule "if the lawyer has made reasonable efforts to prevent the access or disclosure." The comment identifies a number of factors to be considered in determining the reasonableness of the lawyer's efforts. These factors "include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[19] These factors are relied upon by the ABA Standing Committee on Ethics & Professional Responsibility in Formal Opinion 477 (May 2017) to support its conclusion that "it is not always reasonable to rely on the use of unencrypted email."

A lawyer using cloud computing may encounter circumstances that require unique considerations to secure client confidentiality. For example, if a server used by a cloud service provider is physically located in another country, the lawyer must be sure that the data on that server are protected by laws

---

[18] *Id.*

[19] ABA Comment [18] states:

> Acting Competently to Preserve Confidentiality
>
> [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

Similarly, ABA Comment [19], which follows SCR 20:1.6, requires a lawyer, when transmitting a communication that includes information relating to the representation of the client, to take reasonable precautions to prevent the information from coming into the hands of unintended recipients. ABA Comment [19] states:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

that are as protective as those of the United States. Whether a lawyer is required to take additional precautions to protect a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.[20]

**D. SCR 20:5.3 Responsibilities regarding nonlawyer assistants**

Although a lawyer may use nonlawyers outside the firm to help provide legal services, SCR 20:5.3 requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer.[21] The extent of this obligation when using a cloud service provider to process, transmit, store, or access information protected by the duty of confidentiality will depend on the circumstances, including: the education, experience, stability, and reputation of the provider; the nature of the services and information involved; the terms of the arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.[22]

ABA Comment [3], which follows SCR 20:5.3, identifies distinct concerns that arise when services are performed outside the firm. It recognizes that nonlawyer services can take many forms, such as services performed by individuals and services performed by automated products. In addition to identifying the factors that determine the extent of the lawyer's obligations when using such services, it also references other Rules of Professional Conduct that the lawyer should consider when using such services. Comment [3] also emphasizes that the lawyer has an obligation to give appropriate instructions to nonlawyers outside the firm when retaining or directing those nonlawyers. For example, when a lawyer retains an investigative service, the lawyer may not be able to directly supervise how a particular investigator completes an assignment, but the lawyer's instructions must be reasonable under the circumstances to provide reasonable assurance that the investigator's conduct is compatible with the lawyer's professional obligations.[23]

---

[20] ABA Comment [18] to SCR 20:1.6.

[21] SCR 20:5.3 Responsibilities regarding nonlawyer assistants

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

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

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

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

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

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

[22] ABA Comment [3] to SCR 20:5.3.

[23] ABA Comment [3] states:

> [3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this

ABA Comment [4], which follows SCR 20:5.3, recognizes that clients sometimes direct lawyers to use particular nonlawyer service providers.[24] In such situations, the Comment advises that the lawyer should ordinarily consult with the client to determine how the outsourcing arrangement should be structured and who will be responsible for monitoring[25] the performance of the nonlawyer services.

**Part II: Reasonable Efforts**

The Rules of Professional Conduct do not impose a strict liability standard on lawyers who use cloud computing, and none of the ethics opinions require extraordinary efforts or a guarantee that information will not be inadvertently disclosed or that the information will always be accessible when needed.[26] Instead, the Rules require that lawyers act competently to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed, as well as to protect client information from unauthorized access and disclosure, whether intentional or inadvertent. Competency requires the lawyer to make reasonable efforts; and to be reasonable, those efforts must be commensurate with the risk presented.

What constitutes reasonable efforts has been the subject of much discussion. It has been suggested that some of the ethics opinions may place unrealistic demands on attorneys.[27] At the same

---

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

[24] ABA Comment [4] states:

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

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

[26] As one ethics opinion stated: "Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax." N.J. Advisory Committee on Professional Ethics Op. No. 701 (2006).

[27] One expert in the field of data security, Stuart L. Pardau, points out that some ethics opinions, such as Pennsylvania Ethics Op. 2011-200, direct attorneys to negotiate favorable terms of use with the cloud service providers, even though the opinions acknowledge that the providers' terms are usually "take it or leave it" and that a typical attorney is powerless to require a cloud provider to do anything beyond the boilerplate terms. Stuart L. Pardau, "But I'm Just a Lawyer: Do Cloud Ethics Opinions Ask Too Much?" The Professional Lawyer, Vol. 22, Number 4 2014. Pardau also notes that some opinions require attorneys to know

time, it has been suggested that "[i]n sum, basic knowledge of cybersecurity has become an essential lawyer competency."[28]

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

**A. Factors to Consider when Assessing the Risks**

To be reasonable, the lawyer's efforts must be commensurate with the risks presented by the technology involved, the type of practice, and the individual needs of a particular client. The ABA Comments that follow SCR 20:1.6 and 5.3, as well as other ethics opinions, have identified factors for lawyers to consider when assessing the risks. These factors, which are not exclusive, include:

- the information's sensitivity;[29]
- the client's instructions and circumstances;[30]
- the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;[31]

information that they have no practical way of knowing. As examples, Pardau cites Nevada Formal Ethics Op. 33 (2006), which concludes that the attorney will not be responsible for a cloud service provider's breach of confidentiality if the attorney "instructs and requires the third party contractor to keep the information confidential and inaccessible," and New Hampshire Ethics Op. 2012-13/4 opinion, which advises that the attorney "must know at all times where sensitive client information is stored, be it in the cloud or elsewhere." Pardau further observes that "[s]ome of the state bar ethics opinions go too far in requiring attorneys to understand cloud security and monitor providers," citing Alabama Formal Ethics Op. 2010-02, which states that a lawyer has "a continuing duty to stay abreast of the appropriate safeguards that should be employed by … the third-party vendor."

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

[29] ABA Comment [18] to SCR 20:1.6. The more sensitive the information, the less risk an attorney should take.

[30] Calif. Formal Ethics Op. 2010-179 (2010). A lawyer must follow the client's instructions unless doing so would cause the lawyer to violate the Rules of Profession Conduct or other law. Moreover, a lawyer should consider any circumstances that may be relevant. For example, if the attorney is aware that other people have access to the client's devices or accounts and may intercept client information, the attorney should consider that in assessing the risk.

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

- the attorney's ability to assess the technology's level of security;[32]
- the likelihood of disclosure if additional safeguards are not employed;[33]
- the cost of employing additional safeguards;[34]
- the difficulty of implementing the additional safeguards;[35]
- the extent to which the additional safeguards adversely affect the lawyer's ability to represent clients;[36]
- the need for increased accessibility and the urgency of the situation;[37]
- the experience and reputation of the service provider;[38]
- the terms of the agreement with the service provider;[39] and
- the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.[40]

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

**B. General Guidance**

It is impossible to provide specific requirements for reasonable efforts because lawyers' ethical duties are continually evolving as technology changes. Specific requirements would soon become obsolete. Moreover, the risks vary with the technology involved, the type of practice, and the individual

---

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

> Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.

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

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

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

[34] *Id.*

[35] *Id.*

[36] *Id.*

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

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

[39] *Id.*

[40] *Id.*

needs of a particular client.[41] Lawyers must exercise their professional judgment in adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers, and specific requirements would do little to assist the exercise of professional judgment. It is possible, however, to provide some guidance.

- Lawyers should have "at least a base-level comprehension of the technology and the implications of its use."[42] While attorneys are not required to understand precisely how the technology works, competence requires at least a cursory understanding of the technology used. Such a cursory understanding is necessary to explain to the client the advantages and risks of using the technology in the representation.[43]

- Lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication,[44] and encryption for information stored both in the cloud and on the ground.[45] Lawyers should also understand the security dangers of using public Wi-Fi and file sharing sites.

- Lawyers who outsource cloud-computing services should understand the importance of selecting a provider that uses appropriate security protocols. "While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track record prior to utilizing the service."[46] Knowing the qualifications, reputation, and longevity of the cloud-service provider is necessary, just like knowing the qualifications, reputation, and longevity of any other service provider.

- Lawyers should read and understand the cloud-based service provider's terms of use or service agreement.[47]

---

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

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

[43] *Id.*

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

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

[46] Brand at 2.

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

- Ownership of the Information
  Do the terms of use specifically state that the provider has no ownership interest in the information? What happens to the information if the provider goes out of business or if the lawyer decides to terminate the business relationship, or if the lawyer defaults on payments?
- Location of the Information
  Where is information stored? Many providers replicate the information to data centers or servers in other countries with less stringent legal protections. What is the provider's response to government or judicial attempts to obtain client information?
- Security and Confidentiality of Information

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

- Lawyers who do not have the necessary understanding should consult with someone who has the necessary skill and expertise, such as a technology consultant, to help determine what efforts are reasonable.[48]

- Lawyers should also consider including a provision in their engagement agreements or letters that, at the least, informs and explains the use of cloud-based services to process, transmit, store and access information. Including such a provision not only gives the client an opportunity to object, but it also provides an opportunity for the lawyer and client to discuss the advantages and the risks.

**Conclusion**

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

---

What safeguards does the provider have to prevent security breaches? What obligations does the provider have to protect the confidentiality of information? Does the provider agree to promptly notify the lawyer of know security breaches that affect the confidentiality of the lawyer's information?

- Service Level
  Does the service provider have an uptime guarantee? Most providers agree to a 99.9% uptime, although some providers agree to a higher uptime approaching 99.999%.
- Backups
  How frequently does the provider backup the information? How easy is it to restore the information from the backup?
- Disaster Recovery
  Does your provider have a secondary data center or redundant storage that automatically assumes control if disaster strikes the data center or server?

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

> It is also impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's security systems. A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so.

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

## Appendix A
## Cloud Ethics Opinions

**Alabama**
Alabama State Bar Disciplinary Commission
Ala. Ethics Op. 2010-02 (2010)

Lawyers may outsource the storage of client files through cloud computing if reasonable steps are taken to make sure the information is protected. Lawyers must be knowledgeable about how the data will be stored and its security, and must reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Lawyers must also stay abreast of security safeguards.

**Arizona**
State Bar of Arizona Committee on the Rules of Professional Conduct
Ariz. Ethics Op. 09-04 (2009)
Lawyers may use an online file storage and retrieval system that enables clients to access their files as long as the lawyers take reasonable precautions to protect the security and confidentiality of the information. Lawyers must "recogninze their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field." Lawyers must also periodically review the security measures. "If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider."

**California**
State Bar of California Standing Committee on Professional Responsibility and Conduct
Calif. Formal Ethics Op. 2010-179 (2010)
A lawyer's duties of confidentiality and competence require the lawyer to take appropriate steps to ensure that his or her use of technology does not subject client information to an undue risk of unauthorized disclosure. Among the factors to be considered are the technology's level of security, the information's sensitivity, the urgency of the matter, the possible effect inadvertent disclosure or unauthorized interception could pose to a client or third party, as well as client instructions and circimstances. "With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."

**Connecticut**
Connecticut Bar Association Professional Ethics Committee
Conn. Informal Ethics Op. 2013-07(2013)
A "lawyer outsourcing cloud computing tasks (of transmitting, storing and processing data) must exercise reasonable efforts to select a cloud service provider whose conduct is compatible with the professional obligations of the lawyer and is able to limit authorized access to the data, ensure that the data is preserved ('backed up'), reasonably available to the lawyer, and reasonable safe from unauthorized intrusion." The Professional Ethics Committee acknowledged that although the technology examined by it in 1999 might now be obsolete, "the need for a lawyer to thoughtfully and thoroughly evaluate the risks presented by the use of current technology remains as vital as ever." As concluded by the Committee in 1999, the lawyer's efforts must be commensurate with the risk presented. "The lawyer should be satisfied that the cloud service provider's (1) transmission, storage and possession of the data does not diminish the lawyer's ownership of and unfettered accessibility to the data, and (2) security policies and

mechanisms to segregate the lawyer's data and prevent unauthorized access to the data by others including the cloud service provider."

**Florida**

The Florida Bar Professional Ethics Committee
Fla. Ethics Op. 12-3 (2013)
Relying on the New York State Bar Ethics Opinion 842 (2010) and Iowa Ethics Opinion 11-10 (2011), the opinion concludes that lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. Lawyers should research the service provider used and also consider backing up the data elsewhere as a precaution.

**Iowa**

Iowa State Bar Association Committee on Ethics and Practice Guidelines
Iowa Ethics Op. 11-01 (2011)
The opinion concludes that the lawyer is obligated "to perform due diligence to assess the degree of protection that will be needed and to act accordingly." The opinion gives basic guidance by listing questions that the lawyer should ask:

**Accessibility**

1. *Access:*
   Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?
2. *Legal Issues:*
   Have I performed "due diligence regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended by others in the field? What country and state are they located and do business in? Does their end user's licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?
3. *Financial Obligations:*
   What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become property of the SaaS company or is the data destroyed?
4. *Termination:*
   How do I terminate the relationship with the SaaS company? What type of notice does the EULA require? How do I retrieve my data and does the SaaS company retain copies?

**Data Protection**

1. *Password Protection and Public Access:*
   Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?
2. *Data Encryption:*

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

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

**Maine**

Maine State Bar Association Professional Ethics Committee
Maine Ethics Op. 194 (2008)

Lawyers may use third-party electronic back-up and transcription services as long as appropriate safeguards are taken, including reasonable efforts to prevent the disclosure of confidential information, and an agreement with the vendor that contains "a legally enforceable obligation" to maintain the confidentiality of the client's information.

**Massachusetts**

Massachusetts Bar Association Committee on Professional Ethics
Mass. Ethics Op. 12-03 (2012)

A lawyer may generally store and synchronize electronic work files containing client information across different platforms and devices using the Internet as long as the lawyer undertakes reasonable efforts to ensure that the provider's terms of use, privacy policies, practices and procedures are compatible with the Lawyer's professional obligations. Reasonable efforts would include:

> (a) examining the provider's terms of use and written policies and procedures with respect to data privacy and the handling of confidential information;
>
> (b) ensuring that the provider's terms of use and written policies and procedures prohibit unauthorized access to data stored on the provider's system, including access by the provider for any purpose other than conveying or displaying the data to authorized users;
>
> (c) ensuring that the provider's terms of use and written policies and procedures, as well as its functional capabilities, give the Lawyer reasonable access to, and control over, the data stored on the provider's system in the event that the Lawyer's relationship with the provider is interrupted for any reason (e.g., if the storage provider ceases operations or shuts off the Lawyer's account, either temporarily or permanently);
>
> (d) examining the provider's existing practices (including data encryption, password protection, and system backups) and available service history (including reports of known security breaches or "holes") to reasonably ensure that data stored on the provider's system actually will remain confidential, and will not be intentionally or inadvertently disclosed or lost; and
>
> (e) periodically revisiting and reexamining the provider's policies, practices and procedures to ensure that they remain compatible with Lawyer's professional obligations to protect confidential client information reflected in Rule 1.6(a).

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

**Nevada**

State Bar of Nevada Standing Committee on Ethics and Professional Responsibility

Nev. Formal Ethics Op. 33 (2006)
A lawyer may store client files electronically on a remote server controlled by a third party as long as the firm takes reasonable precautions, such as obtaining the third party's agreement to maintain confidentiality, to prevent both accidental and unauthorized disclosure of confidential information.

**New Hampshire**
New Hampshire Bar Association Ethics Committee
N.H. Ethics Op. 2012-13/4 (2013)
A lawyer may use cloud computing consistent with his or her ethical obligations, as long as the lawyer takes reasonable steps to ensure that client information remains confidential. The opinion lists ten issues the lawyer must consider: (1) whether the provider is a reputable organization; (2) whether the provider offers robust security measures; (3) whether the data is stored in a retrievable format; (4) whether the provider commingles data belonging to different clients or different lawyers; (5) whether the provider has a license and not an ownership interest in the data; (6) whether the provider has an enforceable obligation to keep the data confidential; (7) whether the servers are located in the United States; (8) whether the provider will retain the data, and for how long, when representation ends or the agreement between the lawyer and the provider terminates; (9) whether the provider is required to notify the provider if the information is subpoenaed, if the law permits such notice; and (10) whether the provider has a disaster recovery plan with respect to the data.

**New Jersey**
Advisory Committee on Professional Ethics (appointed by the Supreme Court of New Jersey)
N.J. Ethics Op. 701 (2006)
When using electronic filing systems, lawyers must exercise reasonable care against unauthorized access. "The touchstone in using 'reasonable care' against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data."

**New York**
New York State Bar Association Committee on Professional Ethics
N.Y. State Bar Ethics Op. 842 (2010)
A lawyer may use an online computer data storage system to store client files provided "the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained." Reasonable care includes "(1) ensuring that the provider has enforceable obligations to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information; (2) investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances; (3) employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and (4) investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers." In addition, the lawyer should stay informed of both technological advances that could affect confidentiality and changes in the law that could affect any privilege protecting the information.

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

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

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

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

**Ohio**

Ohio State Bar Association Professionalism Committee
Ohio State Bar Association Informal Advisory Op. 2013-03

"[A] lawyer's duty to preserve the confidentiality of cloud-stored client data is to exercise competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive information." When selecting a vendor, it is necessary for the lawyer to know the qualifications, reputation, and longevity of the vendor, and to read and understand the agreement entered into with the vendor. The opinion lists the following "commonly-occurring issues":

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor's part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give "ownership" of the data to the vendor, or is the data merely subject to the vendor's license?
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor's policy regarding returning your client data at termination of its relationship with your firm? What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?

- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

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

**Oregon**

Oregon State Bar Legal Ethics Committee
Or. Ethics Op. 2011-88

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

**Pennsylvania**

Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility
Pa. Ethics Op. 2011-200

A lawyer "may ethically allow client confidential material to be stored in 'the cloud' provided the lawyer takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks." The opinion advises that "[l]awyers may need to consider that at least some data may be too important to risk inclusion in cloud services." The opinion contains a long list of precautions that reasonable care may require.

**Vermont**

Vermont Bar Association
Vt. Advisory Ethics Op. 2010-6 (2011)

Lawyers may use cloud computing in connection with client information as long as they take reasonable precautions to protect the confidentiality of and to ensure access to the information. "Complying with the required level of due diligence will often involve a reasonable understanding of: (a) the vendor's security system; (b) what practical and foreseeable limits, if any, may exist to the lawyer's ability to ensure access to, protection of, and retrieval of the data; (c) the material terms of the user agreement; (d) the vendor's commitment to protecting the confidentiality of the data; (e) the nature and sensitivity of the stored information; (f) notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and (g) other regulatory, compliance and document retention obligations that may apply based upon the nature of the stored data and the lawyer's practice. In addition, the lawyer should consider: (a) giving notice to the client about the proposed method for storing client data; (b) having the vendor's security and access systems reviewed by competent technical personnel; (c) establishing a system for periodic review of the vendor's system to be sure the system remains current with evolving technology and legal requirements; and (d) taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present."

**Virginia**

Virginia Bar Association Standing Committee on Legal Ethics

Va. Legal Ethics Op. 1872 (2013)

"When a lawyer is using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data, the lawyer must follow Rule 1.6(b)(6) and exercise care in the selection of the vendor, have a reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and instruct the vendor to preserve the confidentiality of the information. The lawyer will have to examine the third party provider's use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination." Virginia's Rule 1.6(b)(6) provides that to the extent a lawyer reasonably believes necessary, the lawyer may reveal "information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential."

**Washington**

Washington State Bar Association Rules of Professional Conduct Committee

Wa. Ethics Op. 2215 (2012)

This opinion suggests that the best practices for lawyers "without advanced technological knowledge" would include: "(1) Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession about cloud computing industry standards and features. (2) Evaluation of the provider's practices, reputation, and history. (3) Comparison of provisions in the service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly. (4) Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business. (5) Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer's stored data. (6) Ensure secure and tightly controlled access to the storage system maintained by the service provider. (7) Ensure reasonable measures for secure backup of the data that is maintained by the service provider."

**American Bar Association**

ABA Standing Committee on Ethics & Professional Responsibility

Formal Opinion 477

"[C]yber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email." The opinion does not, however, adopt a bright-line rule prohibiting lawyers from communicating with clients by unencrypted email, which "generally remains an acceptable method of lawyer-client communication." Rather, lawyers "must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable." The opinion admonishes lawyers to understand the nature of the threat by considering "the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion." Lawyers should also "understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information." The opinion emphasizes that it "may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used." However, because deleted data may be subject to

recovery, lawyers "should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all." The opinion also emphasizes the importance of training employees "in the use of reasonably secure methods of electronic communication" and the importance of exercising due diligence in selecting and supervising third-party vendors.