ILLINOIS STATE
BAR ASSOCIATION

Charles J. Northrup
General Counsel

Bailey E. Cunningham
Assistant Counsel

April 11, 2017

Committee Secretary
Supreme Court Rules Committee
222 N. LaSalle Street
13th Floor
Chicago, IL. 60601

Re: ISBA Proposal to Amend the Illinois Supreme Court Rule 769 Committee Comment

Dear Committee Secretary:

On behalf of its more than 32,000 lawyer members, the Illinois State Bar Association ("ISBA") respectfully submits to the Supreme Court Rules Committee a suggested revision to the Committee Comment to Illinois Supreme Court Rule 769 related to electronic storage of lawyer records. The suggested Committee Comment is attached. A referenced ISBA Professional Conduct Advisory Opinion is also attached. The ISBA urges the Committee to review the suggested revision and recommend its inclusion with the Rule to the Court.

Supreme Court Rule 769 addresses a lawyer's duty regarding maintenance of certain practice related records. As the Committee knows, the availability of electronic methods to store these records has increased exponentially over the last several years. The forms of electronic storage have also expanded, with digital media now being very common. As electronic storage methods and forms advance, the costs associated with electronic storage have fallen. As a result, lawyers are turning more and more to electronic storage.

Supreme Court Rule 769 does not mandate any particular records storage method. However, the acceptability of electronic storage is noted in the April, 2003 Committee Comment. The Comment provides that certain forms of electronic storage such as "CDs and DVDs" are appropriate, while other forms such as "floppy disks, tapes, hard drives, zip drives, and other magnetic media" are not. The ISBA believes this Comment is too narrow and does not accommodate the rapid pace of technological change.

In order to provide additional guidance to Illinois lawyers, and to accommodate the likelihood of future technological change, the ISBA is suggesting that the April 2003 Committee Comment be deleted and replaced with the attached new Committee Comment. This suggested new Comment was drafted by the ISBA's Committee on Legal Technology and recently approved by the Board of Governors. The suggested Comment does not dictate any particular electronic storage media, but does note the ability of lawyers to rely on industry standard technology so long as it can meet the Rule's specific storage requirements. The suggested Comment also specifically references an ISBA Professional Conduct Advisory Opinion that provides further detail when lawyers use the "cloud" for storage purposes. That opinion is attached.

In accordance with S.Ct. Rule 3(d) and Administrative Order MR No. 10549, the ISBA requests that the suggested revision be forwarded to the Rules Committee or other appropriate committee for review and appropriate action.

The ISBA appreciates the opportunity to submit this suggested new Committee Comment. If you require any additional information about the proposal, please do not hesitate to contact me.

Very truly yours,

Charles J. Northrup
General Counsel

enclosures

Cc: Jan Zekich (via email)

Rule 769. Maintenance of Records

It shall be the duty of every attorney to maintain originals, copies or computer-generated images of the following:

(1) records which identify the name and last known address of each of the attorney's clients and which reflect whether the representation of the client is ongoing or concluded; and

(2) all financial records related to the attorney's practice, for a period of not less than seven years, including but not limited to bank statements, time and billing records, checks, check stubs, journals, ledgers, audits, financial statements, tax returns and tax reports.

Adopted October 20, 1989, effective November 1, 1989; amended July 18, 1990, effective August 1, 1990 Adopted December 2, 1986, effective January 1, 1987; amended June 12, 1987, effective August 1, 1987; amended November 25, 1987, effective November 25, 1987; amended August 6, 1993, effective immediately; amended October 15, 1993, effective immediately; amended March 26, 2001, effective immediately; amended April 1, 2003, effective immediately; amended ____, 2017, effective immediately.

Committee Comment

(_____, 2017)

As technology and its capabilities rapidly change, this rule addresses the obligations of attorneys and their ability to use digital media or other electronic forms to store their records. It does not dictate the specific media or technology they must use. Attorneys may use industry standard technology that has a reasonable likelihood of providing necessary access capabilities to records for at least seven years. For example, such technology might include online storage or archiving services that provide for long term access, local media such as redundant arrays of inexpensive discs or properly stored optical media, and other existing or future media that can be used onsite or in the cloud which provides a reasonable likelihood of access for seven years or more. Attorneys' obligations when using cloud based services are described in Illinois State Bar Association Professional Conduct Advisory Opinion 16-06 approved by the ISBA Board of Governors in October, 2016. These examples are in no way the only media that conform to this rule. Lawyers must look to use technology industry standards in determining the appropriate technology that complies with this rule and their obligations under it.

~~**Committee Comment**~~
~~**(April 1, 2003)**~~

~~This amendment gives attorneys the option of maintaining records in forms that save space and reduce cost without increasing the risk of premature destruction. For example, CDs and DVDs have a normal life exceeding seven years, so an attorney might use them to maintain financial records. At present, however, floppy disks, tapes, hard drives, zip drives, and other magnetic media have insufficient normal life to meet the requirements of this rule.~~

ISBA Professional Conduct Advisory Opinion

Opinion No. 16-06
October 2016

Subject: Client Files; Confidentiality; Law Firms

Digest: A lawyer may use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer's obligation to protect the client information does not end once the lawyer has selected a reputable provider.

References: Illinois Rules of Professional Conduct, Rules 1.1, 1.6, 5.1 and 5.3

Illinois Rules of Professional Conduct, Rule 1.1, Comment 8 (amended effective Jan. 1, 2016)

ISBA Op. 10-01 (2009)

American Bar Association, Legal Technology Resource Center, www.americanbar.org.

Alabama Ethics Opinion 2010-2 (2010)

Arizona Ethics Op. 09-04 (2009)

Iowa Ethics Opinion 11-01 (2011)

Nevada Formal Opinion No. 33 (2006)

Tennessee Formal Ethics Op. 2015-F-159 (2015)

Washington State Bar Association Advisory Op. 2215 (2012)

FACTS

A lawyer wants to use cloud-based services in her delivery of legal services by contracting with a third party provider. The cloud service will include storage, processing and transmission of information in a shared infrastructure and a shared application, multi-tenant environment. The data will include client personal identifiable information, opposing party documents, financial information, health information and any other confidential and public information relevant to the delivery of legal services. The lawyer plans to conduct due diligence when selecting a third party provider to ensure the controls are in place to maintain confidentiality of the client information and data.

QUESTION

May the lawyer use a third party provider for cloud-based services? If so, is the lawyer's due diligence at the time of entering into an agreement with the provider adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers?

ANALYSIS

Cloud-based services allow a lawyer to store and access software and data in the "cloud," a remote location which is not controlled by the lawyer but is controlled by a third party internet service provider. Lawyers are increasingly choosing to use cloud-based services because the services offer increased flexibility and ease of access to data.

We have previously determined that a lawyer may retain or work with a private vendor to monitor the firm's computer server and network, provided that the lawyer takes reasonable steps to ensure that the vendor protects the confidentiality of client information. *See,* ISBA Op. 10-01 (2009). A similar approach is appropriate when choosing and using cloud-based services. We believe that a lawyer may use cloud-based services. However, because cloud-based services store client data on remote servers outside the lawyer's direct control, the use of such services raises ethics concerns of competence, confidentiality and the proper supervision of non-lawyers.

Rule 1.1 provides that lawyers must provide competent representation to their clients. The Illinois Supreme Court recently amended Comment 8 to Rule 1.1 to provide that as part of a lawyer's duty of competence, lawyers must keep abreast of changes in law and its practice "including the benefits and risks associated with relevant technology." Accordingly, lawyers who use cloud-based services must obtain and maintain a sufficient understanding of the technology they are using to properly assess the risks of unauthorized access and/or disclosures of confidential information.

Lawyers must protect as confidential "all information relating to the representation of the client" pursuant to Rule 1.6. Rule 1.6(e), as recently adopted, provides that a lawyer must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to," confidential information. Factors to be considered in determining the reasonableness of the lawyer's efforts are set forth in Comment 18 to the Rule.

A lawyer's use of an outside provider for cloud-based services is not, in and of itself, a violation of Rule 1.6, provided that the lawyer employs, supervises and oversees the outside provider. *See, e.g.,* Rule 5.3, Comment 3. As stated in a Nevada opinion that discussed a lawyer's use of an outside agency to store electronic client information:

> The use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney's employ. The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a "hacker" who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files. The question in either case is whether the attorney acted reasonable (sic) and competently to protect the confidential information.

Nevada Formal Opinion No. 33 (2006), pp. 2-3.

Because technology changes so rapidly, we decline to provide specific requirements for lawyers when choosing and utilizing an outside provider for cloud-based services. Lawyers must insure that the provider reasonably safeguards client information and, at the same time, allows the attorney access to the data.

At the outset, as recognized by the inquiring lawyer here, lawyers must conduct a due diligence investigation when selecting a provider. Reasonable inquiries and practices could include:

1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
3. Investigating the provider's reputation and history;
4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data;
7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.

Our opinion is consistent with the advisory opinions issued by other state bar associations. Other states that have addressed the issue of cloud computing have also generally concluded that

lawyers may use cloud-based services if they take reasonable steps to protect client information and address the potential risks. *See e.g.,* Alabama Ethics Opinion 2010-2 (2010)(lawyer may outsource storage of client files through cloud computing if the lawyer takes reasonable steps to make sure data is protected); Iowa Ethics Opinion 11-01 (2011)(lawyer should conduct appropriate due diligence before storing files electronically); Tennessee Formal Ethics Opinion 2015-F-159 (2015)(a lawyer may allow client information to be stored in the cloud provided the lawyer takes reasonable care to assure that the information remains confidential and that reasonable safeguards are employed to protect the information from breaches, loss or other risks). *See generally,* "Cloud Ethics Opinions Around the U.S.", American Bar Association, Legal Technology Resource Center, www.americanbar.org.

The inquiring lawyer also asks whether the lawyer's due diligence at the time of entering into an agreement with the provider will be adequate to avoid an ethical violation if a breach of confidentiality should occur through a failure of the provider or through the action of hackers. We do not believe that the lawyer's obligations end when the lawyer selects a reputable provider. Pursuant to Rules 1.6 and 5.3, a lawyer has ongoing obligations to protect the confidentiality of client information and data and to supervise non-lawyers. Future advances in technology may make a lawyer's current reasonable protective measures obsolete. Accordingly, a lawyer must conduct periodic reviews and regularly monitor existing practices to determine if the client information is adequately secured and protected. *See, e.g.,* Arizona Ethics Op. 09-04 (2009); Washington State Bar Association Advisory Op. 2215 (2012).

CONCLUSION

A lawyer may use cloud-based services to store confidential client information provided the attorney uses reasonable care to ensure that client confidentiality is protected and client data is secure. A lawyer must comply with his or her duties of competence in selecting a provider, assessing the risks, reviewing existing practices, and monitoring compliance with the lawyer's professional obligations.
