ILLINOIS STATE BAR ASSOCIATION

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.
