NEW YORK STATE BAR ASSOCIATION
Serving the legal profession and the community since 1876

ETHICS OPINION 1020

New York State Bar Association
Committee on Professional Ethics

Opinion 1020 (9/12/2014)

Topic: Confidentiality; use of cloud storage for purposes of a transaction

Digest: Whether a lawyer to a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

Rules: 1.1, 1.6

FACTS

1. The inquirer is engaged in a real estate practice and is looking into the viability of using an electronic project management tool to help with closings. The technology would allow sellers' attorneys, buyers' attorneys, real estate brokers and mortgage brokers to post and view documents, such as drafts, signed contracts and building financials, all in one central place.

QUESTION

2. May a lawyer representing a party to a transaction use a cloud-based technology so as to post documents and share them with others involved in the transaction?

OPINION

3. The materials that the inquirer seeks to post, such as drafts, contracts and building financials, may well include confidential information of the inquirer's clients, and for purposes of this opinion we assume that they do.[1] Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer's ethical duty to preserve a client's confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client's informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer "exercise reasonable care to prevent … [persons] whose services are utilized by the lawyer from disclosing or using confidential information of a client."

5. Comment [17] to Rule 1.6 addresses issues raised by a lawyer's use of technology:

> 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. The duty 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 use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

6. In the recent past, our Committee has repeatedly been asked to provide guidance on the interplay of technology and confidentiality. N.Y. State 1019 (2014) catalogues the Committee's opinions on technology. In that opinion, we considered whether a law firm could provide its lawyers with remote access to its electronic files. We concluded that a law firm could use remote access "as long as it takes reasonable steps to ensure that confidential information is maintained." Id. ¶12

7. Similarly, in N.Y. State 842 (2010), which considered the use of cloud data storage, we concluded that a lawyer could use this technology to store client records provided that the lawyer takes reasonable care to protect the client's confidential information. We also reached a similar conclusion in N.Y. State 939 (2012) as to the issue of lawyers from different firms sharing a computer system.

8. The concerns presented by the current inquiry were also present in N.Y. State 1019, N.Y. State 939 and N.Y. State 842, and those opinions govern the outcome here. That is, the inquirer may use the proposed technology provided that the lawyer takes reasonable steps to ensure that confidential information is not breached.[2] The inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared. Because of the fact-specific and evolving nature of technology, we do not purport to specify in detail the steps that will constitute reasonable care in any given set of circumstances. See N.Y. State 1019. ¶10. We note, however, that use of electronically stored information may not only require reasonable care to protect that information under Rule 1.6, but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.[3]

9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

CONCLUSION

10. Whether a lawyer for a party in a transaction may post and share documents using a "cloud"

data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

(17-14)

[1]Rule 1.6(a) defines "confidential information" generally to include "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

[2]This result is consistent with results in other jurisdictions that have considered lawyers' use of off-site, third-party cloud services for storing and sharing documents. See, e.g., ABA 95-398; Arizona Opinion 05-04; California Opinion 2010-179; Connecticut Inf. Opinion 2013-07; Florida Opinion 12-3 (2013); Illinois Opinion 10-01 (2009); Iowa Opinion 11-01; Maine Opinion 207 (2013); Massachusetts Opinion 12-03; Massachusetts Opinion 05-04; Missouri Inf. Opinion 2006-0092; Nebraska Opinion 06-05; New Hampshire Opinion 2012-13/4 (2013); New Jersey Opinion 701 (2006); North Carolina Opinion 2011-6 (2012); North Dakota Opinion 99-03 (1999); Ohio Opinion 2013-03; Oregon Opinion 2011-188; Pennsylvania Opinion 2011-200; Pennsylvania Opinion 2010-060; Vermont Opinion 2010-6 (2012); Washington Inf. Opinion 2215 (2012).

[3]It has been said for example that the duty of competence may require litigators, depending on circumstances, to possess a basic or even a more refined understanding of electronically stored information. See, e.g., Zachary Wang, "Ethics and Electronic Discovery: New Medium, Same Problems," 75 Defense Counsel Journal 328, at 7 (October 2008) ("disclosure of privileged information as a result of a lack of knowledge of a client's IT system would subject an attorney to discipline under Rules 1.1 and 1.6"). The California State Bar Standing Committee on Professional Responsibility and Conduct has tentatively approved an interim opinion interpreting California ethical rules as follows:

> Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. … An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

COPRAC Proposed Formal Opinion 11-0004 (2014).

Phone: 518-463-3200 **Secure Fax:** 518.463.5993