NEW YORK STATE BAR ASSOCIATION
NYSBA One Elk Street, Albany, New York 12207 • PH 518.463.3200 • www.nysba.org

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. May a lawyer use an online system to store a client's confidential information without violating the duty of confidentiality or any other duty? If so, what steps should the lawyer take to ensure that the information is sufficiently secure?

OPINION

2. Various companies offer online computer data storage systems that are maintained on an array of Internet servers located around the world. (The array of Internet servers that store the data is often called the "cloud.") A solo practitioner would like to use one of these online "cloud" computer data storage systems to store client confidential information. The lawyer's aim is to ensure that his clients' information will not be lost if something happens to the lawyer's own computers. The online data storage system is password-protected and the data stored in the online system is encrypted.

3. A discussion of confidential information implicates Rule 1.6 of the New York Rules of Professional Conduct (the "Rules"), the general rule governing confidentiality. Rule 1.6(a) provides as follows:

> A lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of a lawyer or a third person, unless:
>
> (1) the client gives informed consent, as defined in Rule 1.0(j);
>
> (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
>
> (3) the disclosure is permitted by paragraph (b).

4. The obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client's confidential information. *See* N.Y. County 733 (2004) (an attorney "must diligently preserve the client's confidences, whether reduced to digital format, paper, or otherwise"). As a New Jersey ethics committee observed, even when a lawyer wants a closed client file to be destroyed, "[s]imply placing the files in the trash would not suffice. Appropriate steps must be taken to ensure that confidential and privileged information remains protected and not available to third parties." New Jersey Opinion (2006), *quoting* New Jersey Opinion 692 (2002).

5. In addition, Rule 1.6(c) provides that an attorney must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except to the extent disclosure is permitted by Rule 1.6(b). Accordingly, a lawyer must take reasonable affirmative steps to guard against the risk of inadvertent disclosure by others who are working under the attorney's supervision or who have been retained by the attorney to assist in providing services to the client. We note, however, that exercising "reasonable care" under Rule 1.6 does not mean that the lawyer guarantees that the information is secure from *any* unauthorized access.

6. To date, no New York ethics opinion has addressed the ethics of *storing* confidential information online. However, in N.Y. State 709 (1998) this Committee addressed the duty to preserve a client's confidential information when *transmitting* such information electronically. Opinion 709 concluded that lawyers may transmit confidential information by e-mail, but cautioned that "lawyers must always act reasonably in choosing to use e-mail for confidential communications." The Committee also warned that the exercise of reasonable care may differ from one case to the next. Accordingly, when a lawyer is on notice that the confidential information being transmitted is "of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer

must select a more secure means of communication than unencrypted Internet e-mail." *See also* Rule 1.6, cmt. 17 (a lawyer "must take reasonable precautions" to prevent information coming into the hands of unintended recipients when transmitting information relating to the representation, but is not required to use special security measures if the means of communicating provides a reasonable expectation of privacy).

7. Ethics advisory opinions in several other states have approved the use of electronic storage of client files provided that sufficient precautions are in place. *See, e.g.*, New Jersey Opinion 701 (2006) (lawyer may use electronic filing system whereby all documents are scanned into a digitized format and entrusted to someone outside the firm provided that the lawyer exercises "reasonable care," which includes entrusting documents to a third party with an enforceable obligation to preserve confidentiality and security, and employing available technology to guard against reasonably foreseeable attempts to infiltrate data); Arizona Opinion 05-04 (2005) (electronic storage of client files is permissible provided lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence"); *see also* Arizona Opinion 09-04 (2009) (lawyer may provide clients with an online file storage and retrieval system that clients may access, provided lawyer takes reasonable precautions to protect security and confidentiality and lawyer periodically reviews security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected).

8. Because the inquiring lawyer will use the online data storage system for the purpose of preserving client information - a purpose both related to the retention and necessary to providing legal services to the client - using the online system is consistent with conduct that this Committee has deemed ethically permissible. *See* N.Y. State 473 (1977) (absent client's objection, lawyer may provide confidential information to outside service agency for legitimate purposes relating to the representation provided that the lawyer exercises care in the selection of the agency and cautions the agency to keep the information confidential); *cf.* NY CPLR 4548 (privileged communication does not lose its privileged character solely because it is communicated by electronic means or because "persons necessary for the delivery or facilitation of such electronic communication may have access to" its contents).

9. We conclude that a lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. "Reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation 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/or

(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.

10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. *See* Rule 1.4 (mandating communication with clients); *see also* N.Y. State 820 (2008) (addressing Web-based email services).

11. Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *See, e.g.*, *City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619, 177 L.Ed.2d 216 (2010) (holding that City did not violate Fourth Amendment when it reviewed transcripts of messages sent and received by police officers on police department pagers); *Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. 2007) (e-mails between hospital employee and his personal attorneys were not privileged because employer's policy regarding computer use and e-mail monitoring stated that employees had no reasonable expectation of privacy in e-mails sent over the employer's e-mail server). *But see Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 990 A.2d 650 (2010) (despite employer's e-mail policy stating that company had right to review and disclose all information on "the company's media systems and services" and that e-mails were "not to be considered private or personal" to any employees, company violated employee's attorney-client privilege by reviewing e-mails sent to employee's personal attorney on employer's laptop through employee's personal, password-protected e-mail account).

12. This Committee's prior opinions have addressed the disclosure of confidential information in metadata and the perils of practicing law over the Internet. We have noted in those opinions that the duty to "exercise reasonable care" to prevent disclosure of confidential information "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks" in transmitting information electronically. N.Y. State 782 (2004), *citing* N.Y. State 709 (1998) (when conducting trademark practice over the Internet, lawyer had duty to "stay abreast of this evolving

technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost"); *see also* N.Y. State 820 (2008) (same in context of using e-mail service provider that scans e-mails to generate computer advertising). The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.

CONCLUSION

13. A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.

(75-09)