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

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, *e.g.:*

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102(D) [now Rule 1.15(d)].
N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.
N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".
N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.
N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.
N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.
N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.
N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not

knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

> [17] 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 to 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.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also noted, however, that "when the confidential information 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." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving the use of "cloud" data storage, we were told that the storage system was password protected and that data stored in the system was encrypted. We concluded that the lawyer could

use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "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.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, Locked Down: Information Security for Lawyers (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that 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.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses 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).

7-14