ILLINOIS STATE BAR ASSOCIATION

ISBA Advisory Opinion on Professional Conduct

ISBA Advisory Opinions on Professional Conduct are prepared as an educational service to members of the ISBA. While the Opinions express the ISBA interpretation of the Illinois Rules of Professional Conduct and other relevant materials in response to a specific hypothesized fact situation, they do not have the weight of law and should not be relied upon as a substitute for individual legal advice.

This Opinion was AFFIRMED by the Board of Governors in January 2010. This opinion was affirmed based on its general consistency with the 2010 Rules, although the specific standards referenced in it may be different from the 2010 Rules. Readers are encouraged to review and consider other applicable Rules and Comments, as well as any applicable case law or disciplinary decisions.

Opinion No. 10-01
July 2009

Topic: Law firm's maintenance of confidential information while working with third-party technology vendor

Digest: A law firm's utilization of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information

Ref.: Illinois Rules of Professional Conduct Rules 1.6(a), 5.3, 1.4(b)

ISBA Advisory Opinion No. 03-07 (May 2004)

ISBA Advisory Opinion No. 96-10 (May 1997)

ABA Formal Opinion Nos. 95-398 (Oct. 27, 1995), 08-451 (Aug. 5, 2008); 99-413 (March 10, 1999).

In re Estate of Divine, 263 Ill. App. 3d 799, 635 N.E.2d 581 (1st Dist. 1994)

Massachusetts Bar Association Ethics Opinion No. 05-04

Restatement (Third) of the Law Governing Lawyers § 60 (2000)

Electronic Communications Privacy Act, 18 U.S.C. § 2510

FACTS

A law firm would like to have its computer network managed by an off-site third party vendor for the purpose of monitoring the server and responding to any problems which may develop on the firm's network. In order to respond to such problems, the vendor would need to have access to the firm's network in which electronic client files are stored. The sole purpose of the vendor's access to the network would be for administration of the computer system. Moreover, the law firm and vendor would enter into a written agreement whereby the vendor would agree to respect and maintain the confidentiality of the information within the network, and to not utilize or disclose it.

QUESTIONS

1. What ethical issues should be considered if a law firm utilizes an off-site network administrator to assist in the operation of the law practice if the firm's server were located at the firm and the vendor had remote access, or alternatively, if the server were physically located at the vendor?

2. Would either arrangement violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information?

OPINION

The ethical issues that should be considered if a law firm utilizes an off-site network administrator to assist in the operation of its law practice principally involve two of the Illinois Rules of Professional Conduct ("RPC"): RPC 1.6(a) and 5.3.

RPC 1.6(a), entitled, "Confidentiality of Information," provides:

> Except when required under Rule 1.6(b) or permitted under Rule 1.6(c), a lawyer shall not, during or after termination of the professional relationship with the client, use or reveal a confidence or secret of the client known to the lawyer unless the client consents after disclosure.

The RPC's define "confidence" as "information protected by the lawyer-client privilege under applicable law."

RPC 5.3, entitled, "Responsibilities Regarding Nonlawyer Assistants," provides:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:

> (a) The lawyer, and, in a law firm, each partner, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer and the firm;
>
> (b) each lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the nonlawyer's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for a nonlawyer's conduct that would be a violation of these Rules if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner in the law firm, or has direct supervisory authority over the nonlawyer, and knows of the nonlawyer's conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Here, because the offsite third-party computer vendor ("Vendor"), a nonlawyer, would have access to client files when monitoring and administering the law firm's network, the contents of these files must be protected from disclosure under RPC's 1.6(a) and 5.3. Thus, the law firm giving access to the Vendor to information in client files must make reasonable efforts to ensure that the Vendor either has in place or will institute reasonable procedures to safeguard the confidentiality of the client information.

This same scenario was addressed by the American Bar Association ("ABA") in Formal Op. 95-398, wherein the ABA acknowledged that in this age of rapidly developing technology, it is now commonplace to retain nonlawyers to perform numerous functions, including accounting, data processing and storage, printing, photocopying, computer servicing and paper disposal. Because the use of such outside service providers inevitably requires giving them access to client files, lawyers must make reasonable efforts to ensure that the service provider will not make unauthorized disclosures of client information. ABA Op. 95-398. To that end, the law firm should obtain from the Vendor a written statement of the Vendor's assurance of confidentiality with respect to the electronic client files stored on the network. ABA Op. 95-398. The ABA subsequently issued Formal Op. 08-451 (Aug. 5, 2008), in which it remarked that there is "nothing unethical about a lawyer outsourcing" nonlegal services, including the use of a third-party vendor to maintain a law firm's computer system, but warned that the lawyer must minimize the risk that the outside service provider may inadvertently reveal confidential client information. The ABA reiterated its opinion that written confidentiality agreements are strongly advisable in outsourcing relationships. ABA Op. 08-451. *See also* ISBA Formal Op. 03-07 (May 2004) (opining that the responsibilities of lawyers regarding nonlawyer assistants extends to interpreters who are retained by the lawyer to communicate with hearing impaired clients, including the protection of client confidences).

In addition, the ABA observed that in the event the Vendor breaches the confidentiality of the firm's client files, a lawyer may be obligated to disclose this breach to its client if it is likely to affect the position of the client or the outcome of the client's case. Such disclosure may be required under RPC 1.4(b), pursuant to which a "lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." ABA Op. 95-398. *See also In re Estate of Divine*, 263 Ill. App. 3d 799, 808 (1st Dist. 1994) (observing that RPC 5.3 places the responsibility for unethical acts by nonlawyer employees on the employing attorney). Other laws may also require disclosure to the client, such as notification about a data security breach.

The ABA Formal Opinions cited herein are consistent with other authorities which have addressed the issue of the lawyer's duty to safeguard client confidentiality when dealing with outside service providers. For example, Massachusetts Bar Association Ethics Opinion 05-04 ("MBA 05-04") involved a situation in which a vendor periodically accessed a law firm's computer system, including its server and document database, in order to support the firm's computer software application. The MBA concluded that this practice was reasonable and did not violate any ethical rules:

> We believe that it is well known among the general population that computer systems are an integral and essential tool of the modern-day legal profession, and that those computer systems, and the software that they operate, must be made available to technicians and other trained support personnel more often than we desire for the purpose of keeping them running. It would be impractical and unrealistic to expect a lawyer to delete or 'scrub' all confidential client information from his or her computer before allowing it to be serviced. Indeed, in circumstances where the system has failed unexpectedly and completely, it may be physically impossible for the lawyer to do so.

MBA 05-04. However, the MBA opined that the lawyer must take reasonable steps to protect its clients' confidential information, examples of which include: "notifying the vendor of the confidential nature of the information stored on the firm's servers and in its document database; examining the vendor's existing policies and procedures with respect to the handling of confidential information; obtaining written assurance from the vendor that access is only for technical support purposes and that the system will only be accessed on an as needed basis; and obtaining written assurance that the vendor will preserve and protect all client information." MBA 05-04.

Likewise, Restatement (Third) of Law Governing Lawyers § 60 (Comment d) (2000) ("Comment d") provides that a lawyer who acquires confidential client information has a duty to take reasonable steps to secure the information against misuse or inappropriate disclosure by the lawyer's agents. "This requires that client confidential information be acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality." Comment d. Further, Restatement Comment g provides that a "lawyer may disclose confidential client information for the purpose of facilitating the lawyer's law practice," including to computer technicians, provided that the lawyer takes "appropriate safeguards against impermissible use or disclosure."

Finally, whether the Vendor has physical or remote access to the law firm's server is irrelevant so long as other adequate safeguards are taken.. The ABA has opined that the communication of confidential client information over the internet, even by unencrypted email, does not violate Rule 1.6. ABA Formal Op. 99-413 (1999). Moreover, internet users, including lawyers, have a reasonable expectation that communications will remain private. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2510; ISBA Ethics Advisory Opinion 96-10. Consequently, it makes no difference whether the Vendor in the fact scenario presented has remote or on-site access to the law firm's network.

CONCLUSION

Under RPC's 1.6 and 5.3, a law firm may retain or work with a private vendor to monitor the firm's computer server and network, either on-site or remotely, and may allow the vendor to access it as needed for maintenance, updating, troubleshooting and similar purposes. Before doing so, however, the law firm must take reasonable steps to ensure that the vendor protects the confidentiality of the clients' information on the server.