

# Chicago Daily Law Bulletin®

Volume 163, No. 97

Serving Chicago's legal community for 162 years

## New ABA communications guidelines looks for 21st century update

In a significant opinion published last week, the American Bar Association's Standing Committee on Ethics and Professional Responsibility provided additional guidance on a lawyer's obligations to protect client confidentiality in electronic communications.

Formal Ethics Opinion 477 updates an outdated 1999 opinion on encrypted communications, which provided generally that a lawyer could, without violating his or her obligations of confidentiality, transmit confidential client information through unencrypted e-mails, since, at the time, "the mode of transmission afford[ed] a reasonable expectation of privacy from a technological and legal standpoint."

The intervening 18 years brought both significant technological advances as well as new and increasingly sophisticated ways that our (and our clients') communications and other data can be breached by outside actors.

Moreover, in 2012, the ABA adopted the "technology amendments" to the Model Rules, which provided lawyers with new guidelines for technical competencies. The Illinois Supreme Court subsequently approved that language, which now appears in the Illinois Rules of Professional Conduct.

The standing committee's new opinion focuses on three key areas of a lawyer's professional obligations and how each is impacted by today's technological environment: (a) the duty of confidentiality under Rule 1.6, (b) the duty of competence

under Rule 1.1 and (c) the duty to communicate under Rule 1.4.

The majority of the standing committee's opinion is devoted to what is perhaps the most important of ethics rules: a lawyer's duty of confidentiality.

As the standing committee noted, the 2012 rule amendments added Amended Comment 18 to Rule 1.6, which provides that lawyers have an affirmative duty to "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer."

Functionally, that means that lawyers must exercise "reasonable efforts" to safeguard confidentiality when using electronic communications. The standing committee

*The standing committee rejected a hard and fast rule regarding what it means to use reasonable efforts, instead favoring a fact-specific analysis to be employed on a case-by-case basis.*

rejected a hard and fast rule regarding what it means to use reasonable efforts, instead favoring a fact-specific analysis to be employed on a case-by-case basis.

To aid lawyers in determining what "reasonable efforts" includes in any particular situation, the standing committee provided a list of nonexclusive factors to consider.

Those factors include: (a) the sensitivity of the information be-

### BY TRISHA M. RICH

*Trisha M. Rich is a commercial litigator and professional responsibility lawyer in Holland & Knight LLP's Chicago office. She can be reached at trisha.rich@hkllaw.com or at (312) 578-6514.*

ing sent, (b) the likelihood that the information would be disclosed in the absence of additional safeguards, (c) the cost of employing additional safeguards and (d) the extent to which the additional safeguards would encumber the lawyer's ability to effectively represent his or her clients.

By way of example, the standing committee noted for matters of normal or low sensitivity, the reasonable efforts standard may be met with standard security measures; indeed, it specifically notes

lawyers have a duty to stay abreast of technological advances. Model Rule 1.1 Comment 8.

The opinion relies on guidance from the ABA Commission on Ethics 20/20 to provide that "lawyers necessarily need to understand basic features of relevant technology."

Finally, under Model Rule 1.4, lawyers have an affirmative duty to promptly communicate material developments to clients as well as to keep clients reasonably informed about the progress of their matters.

In its new opinion, the standing committee noted that in cases where the lawyer reasonably believes that a communication includes highly sensitive confidential client information and thus warrants extra security measures, the lawyer should inform the client about the risks involved and decide together with the client whether another form of communication would be better suited to transmitting the pertinent information.

Formal Ethics Opinion 477 is an important update that provides lawyers with guidance on how to properly protect client data and communications.

While lawyers can continue to transmit client information electronically, lawyers need to be aware that special security precautions may be required in circumstances where it is required by law, by a client or where the information being transmitted requires a higher degree of security and protection.