

**ORR & RENO, P.A. ETHICS AND PROFESSIONAL LIABILITY  
QUARTERLY REVIEW (October 2011)**

**The Ethics of Conducting Privileged Communications with Clients  
Using Their Workplace Computers**

Orr & Reno's 2011 First Quarterly Review, *The Ethics of Using Technology in Legal Representation* (January 2011), addressed the importance of maintaining confidentiality while communicating with clients electronically. We highlighted the importance of taking precautions to prevent unintended third parties from accessing transmitted information and cited typical precautions to prevent access by unknown third parties, e.g., encryption, firewalls and anti-virus software. However, attorneys also should consider the risks of access by a third party associated with the client. This situation may arise in a variety of contexts, but perhaps the most prevalent involves a client's use of his or her workplace computer and/or email account to communicate privileged information to an attorney. Many employers are authorized by internal policy to access and monitor employees' computers and emails. Because there is a risk that such communications would be accessible to a third party, lawyers must consider this risk when communicating with clients.

Rule 1.6 of the New Hampshire Rules of Professional Conduct generally prohibits an attorney from revealing to any third party information related to representation of a client, with limited exceptions. The American Bar Association (ABA) comments on Model Rule 1.6 state that "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." *See* N.H. R. Prof. C. 1.6, 2004 ABA Model Code Comment [17]. A recently issued ABA Formal Opinion sheds further light on a lawyer's obligation to take "reasonable precautions" in complying with Rule 1.6. *See* ABA Formal Opinion 11-459 (Aug. 4, 2011). The August 4, 2011 ABA Opinion is based upon the following circumstances: an employee contacted an attorney for advice regarding a potential claim against her employer. She used her workplace computer and email account to communicate with the attorney about her claim. The employer had an internal policy granting a right of access to all employees' computers and email files.

The ABA concluded that an attorney is typically obligated to instruct a client to avoid using a workplace system for sensitive or substantive communications (and possibly any attorney-client communications), at least where there is a risk of harm to the client. According to the ABA, the duty to instruct the client arises when the lawyer knows, or reasonably should know, that the client is likely to send or receive substantive attorney-client communications where there is a significant risk that the communication will be read by the employer (or other third party). A lawyer should ordinarily assume that an employer's internal policy allows for access to the employee's emails sent or received by a workplace device. Consequently, in such situations, an attorney should refrain from sending emails to a client's workplace email account, and should caution the client against using a business email account, or accessing a personal email account from

a workplace computer, when communicating substantive information regarding the representation.

*The Quarterly Review is intended to provide a general overview of current legal ethics issues. It is not, and should not be construed, as legal counsel or advice. If you would like more information from a member of the Ethics and Professional Liability Practice Group, please contact a member of our [practice group](#).*