Schnader | The Higher Calling of the Law

Published in The Legal Intelligencer – https://www.law.com/thelegalintelligencer/2021/07/14/ethical-issues-presented-by-cyber-tech-in-attorney-client-communications/

Ethical Issues Presented by Cyber Tech in Attorney-Client Communications

By Michael J. Wietrzychowski and Brian Clarke | July 14, 2021

The use of technology in a law office or legal department raises many ethical issues concerning how confidential and privileged electronic information must be stored, shared, and protected. These issues are heightened where attorneys and staff work remotely, as the protections that such information may enjoy in the traditional office setting may not exist at the home office or other remote location.

This article provides pointers on maintaining confidentiality and avoiding inadvertent disclosure by ensuring communications and data remain privileged and protecting against breaches and loss.

ETHICS RULES

Pennsylvania requires that when working remotely, attorneys and staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to ensure:

- Telephone calls, text messages, email, video conferencing, and all other communications are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Use of the internet and information transmitted through the internet are handled in a manner that ensures the confidentiality of client communications and other sensitive data;
- Remote work settings are designed and implemented to prevent the disclosure of confidential information in both paper and electronic form;
- Proper procedures are used to secure and back up confidential data stored on electronic devices and in the cloud;
- Appropriate forms of overall data security are utilized; and
- Attorneys and staff working remotely are informed about and have the resources to make their work compliant with the Rules of Professional Conduct.

The Rules of Professional Conduct relevant to these various considerations include, among others:

- Rule 1.1 Competence—"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology …"

- Rule 1.6 Confidentiality of Information—"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

BEST PRACTICES

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility provides a list of "appropriate measures" for attorneys to consider to protect confidential electronic communications both inside and outside of the office. These measures include:

Establishing how and where data will be stored and how the data will be backed up. Most law firms and legal departments should have robust backup systems, as well as software for organizing the totality of the electronic data for the client, such as a document management system. Saving client data on personal devices comes with a number of risks as the data is now stored permanently on the lawyer's home computer and network, and could be easily lost due to a hardware failure or data breach.

Assessing and securing the home network. Law firms and legal departments generally have a multitude of tools for knowing what devices are on their network and limiting access to confidential client data on a "need to know" basis. Firewalls and advanced anti-virus technologies can prevent intrusions from malicious actors who would seek to encrypt and/or steal client data. Identifying the various devices that are on your home network and what activity is going on should be on the mind of every attorney working remotely. The most common activities, such as streaming videos or playing online games, are low risk. However, all manner of questionable websites, as well as video sharing sites, may be accessed from a variety of devices owned by family members using the attorney's home network. Thus, the devices can be compromised and used by an attacker to look for other devices on the network to infect.

Using firewalls, anti-virus and anti-malware software, and other similar products. Make sure that your personal device has firewalls, anti-virus and anti-malware software installed, and be cautious about where you go online. In addition, you should be familiar with the supported lifecycle of your device. While laptops and desktop computers could have a lifecycle of 10 years or more, it is likely that the operating system, whether Mac or Windows, may stop receiving security updates as the system ages. At that point, the system is considered especially vulnerable to malware attacks and should no longer be used, especially for working with confidential client data. While it may be tempting to stretch another year of life out of an expensive hardware item, make sure that your device and the software you use are supported with current security updates.

Using two-factor authentication or similar safeguards. Phishing attacks are very common, and network credentials can be very easily stolen in a phishing attack unless two-factor authentication is used. Once attackers have access to an e-mail account, they can exfiltrate or at least read confidential client communications. For example, there have been many cases of financial fraud where a malicious actor used a compromised e-mail account to send new banking

instructions at the conclusion of a legal transaction. While it is important to safeguard your own e-mail account with two-factor authentication, you should be aware that not everyone does. Take extra care when sending extremely confidential information to clients and confirm any details for wiring money by telephone.

Prohibiting the use of public or free Wi-Fi. When away from your home network (which should of course be secured and the password not shared outside your home), take care to not connect to public hotspots to conduct client work. Consider using a MiFi hotspot or the hotspot function on your phone to create a Wi-Fi connection for your computer to perform client work. Sophisticated threat actors can create Wi-Fi connections that mimic coffee shop and even hotel Wi-Fi networks. While the risks of snooping are relatively low if the connection to your office's network is encrypted, recognize that network security is not a priority on a guest network, as it is within your office's network.

Implementing policies and training attorneys and staff handling confidential electronic information. Safeguards are ineffective unless law offices and legal departments invest in the implementation and training needed for employees to adhere to them. At a minimum, offices should implement and distribute policies dictating the conditions for handling confidential information away from the office. Offices should receive written acknowledgment from persons possessing confidential information stating that they agree to abide by the terms of applicable policies. Offices may want to consider "auditing" remote workspaces to ensure that they are set up in a way to handle confidential electronic information securely. Offices also should train employees on the details of securing information. Other training and practices could include providing "phishing" tests to keep employees sharp, requiring passwords to be "strong" and changed frequently, and limiting the information that may be handled remotely, as well as specifying which persons may use the information.

CONCLUSION

It is every attorney's duty to protect and secure client information both in the office and at home. Attorneys are ethically obligated to ensure that electronic information is stored and shared in a manner that is safe and up-to-date.

The importance of these issues has been further increased by the remote working conditions of the COVID-19 pandemic, which are expected to continue even as offices reopen. The Pennsylvania Rules of Professional Conduct emphasize the necessity for attorneys to address these ethical and technology concerns.

==========

Michael J. Wietrzychowski is co-chair of Schnader Harrison Segal & Lewis' labor and employment practices group. Contact him at mwietrzychowski@schnader.com.

Brian Clarke is director of information services at the firm. Contact him at bclarke@schnader.com.