Alert

March 30, 2020

COZEN O'CONNOR

Ethical Issues with Remote Work During COVID-19

Deborah Winokur

Associate
General Counsel
– Professional
Responsibility

dwinokur@cozen.com
Phone: (215) 665-4195
Fax: (215) 701-2022

Related Practice Areas

- Legal Profession Services
- Technology, Privacy & Data Security

International and national events have triggered an immediate and emergent need for employers to transition their entire work force to working remotely. The World Health Organization officially declared the novel coronavirus outbreak a pandemic on March 11, and President Donald Trump declared a national emergency on March 13. Federal, state, and local regulations are in a state of flux with 16 states implementing shutdown orders, halting in-person business operations. In Pennsylvania, Governor Wolf dodged a constitutional challenge to his shutdown order of "non-essential" businesses by modifying it to permit law offices to stay open on a restricted basis. Per the Pennsylvania Office of General Counsel's guidance, lawyers and their staff may access their offices to the degree necessary to participate in essential court functions. The guidance reiterates that all other businesses must continue to operate remotely. Businesses in regions where shutdown orders have not been issued (yet) are taking measures to protect the health and safety of their employees, customers, and operations. As widely recognized, "[o]ne of the key measures to reduce the spread of Coronavirus COVID-19 is social distancing, which for many organizations means encouraging — or instructing — staff to work from home." Steve Ranger, "Working from home: Cybersecurity tips for remote workers" (March 16, 2020).

For employers the rapid migration of workers to a remote environment triggers a host of potential operational, employment, and legal ethical issues. From a business operations standpoint, companies need to be prepared to take necessary measures to maintain and manage critical functions remotely, which may include altering supply chains or suspending certain operations, as well as coordinating and communicating directly with customers. These companies should identify key personnel to manage both the internal response to employees and coordinate with third-parties, including customers and vendors.

The following Alert will address some of the legal ethical issues employers are facing while their businesses are operating remotely. We will also touch on ethical issues with outsourcing legal services and cybersecurity in and out of the office.

Even amidst a crisis, lawyers are bound by their ethical obligations and must protect their clients' interests in pending matters. (*See* ABA Special Committee on Disaster Response and Preparedness (February 12, 2011), and note Model Rule 1.1, Comment [3] regarding an emergency). Lawyers must continue to competently and diligently represent clients, communicate relevant information, safeguard clients' confidential information, comply with court issued filing deadlines and appear remotely for court appearances, and fulfill fiduciary duties regarding safekeeping of client property. Law firms should have business continuity plans (BCPs) in place that address how to continue carrying out critical business operations during or immediately after a disaster. Even if a law firm does not have a current BCP, there are a number of steps firms can take to comply with their ethical obligations and mitigate risk. The ABA Special Committee advises that law firms take the following steps in the event of an emergency:

1. Create internal and external messaging regarding the firm's status and ability to operate;
2. Coordinate with records management to ensure that incoming documents are being stored securely and that records are accessible as necessary;
3. Ensure that attorneys are performing analyses to identify and prioritize urgent matters, including docketing litigation deadlines and court appearances; and
4. Identify firm leadership responsible for responding to questions about essential firm functions.

(*See, Surviving a Disaster: A Lawyer's Guide to Disaster Planning* (2011)).

With the spread of COVID-19, many firms are outsourcing various legal services. Outsourcing

generally refers to “the practice of taking a specific task or function previously performed within a firm or entity and, for reasons including cost and efficiency, having it performed by an outside service provider.” *See* ABA Commission on Ethics 20/20, *Revised Proposal — Outsourcing* (Sept. 19, 2001). Contract lawyers may perform legal research, prepare briefs, review discovery material, and make court appearances. Third-party vendors can perform document management and review, transcription, and legal research, and assist in developing case strategies. Due to the COVID-19 pandemic, additional reasons for outsourcing include the need for social distancing and the necessity of firms working remotely.

Outsourcing is not a novel concept and there are significant ethical issues to be considered when retaining outside counsel and third-party vendors to handle certain aspects of a firm’s legal work. There are ethical implications to hiring a lawyer, whether deemed of counsel, associated, or a contract lawyer. There are also ethical implications to outsourcing other aspects of a law firm’s work, such as accounting and bookkeeping, receptionists, information technology support, advertising and marketing, and paralegal tasks. As practices become more specialized and support options proliferate, even more activities traditionally handled by lawyers may come to be outsourced in the future.

The principle at the heart of the ethics issues is this: the attorney choosing to outsource work bears ultimate responsibility for her work and that responsibility cannot be delegated. *See* Fla. Bar Ethics Op. 07-2 (Jan. 18, 2008); Kentucky Bar Ethics Op. E-142 (Mar. 1976). ABA Formal Op. 08-451 (August 5, 2008) states:

> A lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under Model Rule 1.1. In complying with her Rule 1.1 obligations, a lawyer who engages lawyers or nonlawyers to provide outsourced legal or nonlegal services is required to comply with Rules 5.1 and 5.3. She should make reasonable efforts to ensure that the conduct of the lawyers or nonlawyers to whom tasks are outsourced is compatible with her own professional obligations as a lawyer with “direct supervisory authority” over them.
>
> In addition, appropriate disclosures should be made to the client regarding the use of lawyers or nonlawyers outside of the lawyer’s firm, and client consent should be obtained if those lawyers or nonlawyers will be receiving information protected by Rule 1.6. The fees charged must be reasonable and otherwise in compliance with Rule 1.5, and the outsourcing lawyer must avoid assisting the unauthorized practice of law under Rule 5.5.

Lawyers engaged in the outsourcing of substantive legal work must consider their ethical obligations to do the following: (1) ensure competence and appropriate supervision; (2) preserve the client’s confidential information; (3) check for conflicts of interest; (4) disclose the outsourcing arrangement to the client; and (5) avoid assisting in the unauthorized practice of law.

Competence and Supervision

Lawyers have a duty to act competently in the representation of clients, and to ensure that those who are working under their supervision perform competently. Model Rule 1.1 requires that an attorney provide competent representation, which requires “the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” Work performed on a client matter by an outsourced provider must ultimately contribute to a “competent” representation.

To satisfy the duty of competence, a lawyer who outsources work must ensure that the tasks in question are delegated to individuals who possess the skills required to perform them, and that the individuals are appropriately supervised to ensure competent representation of the client. *See* ABA Op. 08-451 (August 5, 2008). Ensuring that an outsourced provider contributes to a “competent” representation can largely be accomplished by how the provider is supervised.

Under Model Rules 5.1 and 5.3 an outsourcing attorney has the responsibility to require the ethical conduct of lawyers and non-lawyers under the attorney’s supervision. For lawyers, the attorney must take reasonable efforts to ensure their conduct “conforms” to the Model Rules under Rule 5.1(b); for non-lawyers the attorney must take reasonable efforts to ensure their conduct is “compatible with” the Model Rules under Rule 5.3(a). With both lawyers and non-lawyers, a supervising attorney has committed an ethics violation if she orders or ratifies conduct that

constitutes a rule violation, Model Rule 5.1(c) and 5.3(c)(1).

Preservation of Client Confidential Information

One of a lawyer's core ethical duties, of course, is to safeguard her client's information. In the digital era, much of the attention on this fundamental duty has appropriately centered on issues involving lawyers' use of technology. Just as a lawyer has a responsibility to vet the use of technologies deployed for use within a firm, she has a responsibility to vet an outsourced provider to ensure that client data will be protected from a technological, procedural, and legal standpoint. These are serious yet surmountable challenges.

The lawyer's duty to secure client information is outlined in Model Rule 1.6 and the responsibility to maintain client confidences, together with Model Rule 1.1. Under Model Rule 1.6, a lawyer must take appropriate steps to ensure that client information is not disclosed by an outsourced provider, whether accidentally or intentionally. The comment to Model Rule 1.6(c):

> requires a lawyer 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 or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

Data security is one of the most serious ethics concerns with outsourced providers. At a minimum, a lawyer outsourcing services for ultimate provision to a client should consider conducting reference checks and investigating the background of the lawyer or non-lawyer providing the services as well as any non-lawyer intermediary involved, such as a placement agency or service provider. The lawyer also might consider interviewing the principal lawyers, if any, involved in the project, among other things assessing their educational background and pertinent experience. When dealing with an intermediary, the lawyer may wish to inquire into its hiring practices to evaluate the quality and character of the employees likely to have access to client information. Depending on the sensitivity of the information being provided to the service provider, the lawyer should consider investigating the security of the provider's premises, computer network, and perhaps even its recycling and refuse disposal procedures. In some instances, it may be prudent to pay a personal visit to the intermediary's facility, regardless of its location or the difficulty of travel, to get a firsthand sense of its operation and the professionalism of the lawyers and non-lawyers it is procuring.

Conflicts of Interest

Ethics committees unanimously agree that law firms must guard against conflicts of interest when using outsourced providers. Lawyers must adhere to the strict and well-known rules governing conflicts of interest. But the rules do not directly apply to non-lawyers. Instead, under Model Rule 5.3, non-lawyers within a firm must act in a way that is "compatible" with the lawyers' obligations, including to screen for conflicts. This entails responsibility on the outsourcing attorney to screen outsourced providers for conflicts.

The ABA advises that the outsourced provider must not work for adversaries of clients "on the same or substantially related matters." *See* ABA Formal Op. 08-451, *supra* note 1, at 5. This language invokes the legal standard applicable to duties owed to former clients: an attorney cannot represent a new client in "the same or a substantially related matter" to the former client's representation. *See* Model Rule 1.9(a).

Commentators and ethics opinions agree that attorneys have a duty to take steps to avoid conflicts. *See* NYC Bar Ethics Op. 2006-3 (Aug. 2006), note 9. The firm and its outsourced provider must have a mechanism in place to screen for conflicts. It may be wise to have the outsourced provider complete a conflict check questionnaire to memorialize that the check was performed. *See* NYC Bar Ass'n Comm. On Prof. Resp., *Report on the Outsourcing of Legal Services Overseas* (2007).

Client Disclosure/Client Consent

Model Rule 1.6 prohibits an attorney from revealing information "relating to the representation of a client" absent informed consent or implied authorization from the client. *See* Model Rule 1.6(a). The

scope of Rule 1.6 is broad enough to encompass virtually any information received from a client during a legal representation. The prevailing view is that an attorney must secure informed consent to release confidential information to an outsourced provider. *See* ABA Formal Op. 08-451, *supra*, note 1, at 5.

The ABA has opined that a client impliedly consents to disclosure of information with contract attorneys working within a firm, but concludes the more attenuated supervision and control makes outsourced providers qualitatively different. *Id*. There is no "convenience" exception to Model Rule 1.6.

Unauthorized Practice of Law

Model Rule 5.5 prohibits a lawyer from assisting in the unauthorized practice of law (UPL). Likewise, under Model Rule 8.4 it is misconduct for a lawyer to "knowingly assist or induce another" to violate the rules of conduct. *See* Model Rule 8.4(a). The question of whether a particular activity constitutes the practice of law is not itself an ethics question, but rather depends on the regulatory law of a particular jurisdiction. *See* Preamble to Model Rules.

Addressing the issue, the New York City Bar Association cautions that lawyers who retain outsourced providers must remain at the helm of the representation

> ... to avoid aiding the unauthorized practice of law, the lawyer must at every step shoulder complete responsibility for the non-lawyer's work. In short, the lawyer must, by applying professional skill and judgment, first set the appropriate scope for the non-lawyer's work and then vet the non-lawyer's work and ensure its quality.

See NYC Bar Ethics Op. 2006-3, note 9.

The hiring lawyer must remain responsible for decisions on the representation and must appropriately supervise work by non-lawyers. At the end of the day, the hiring lawyer must remain the lawyer: fully in charge of the representation. The prohibition against UPL is no inherent bar to the use of outsourced providers so long as the hiring lawyer remains the lawyer.

There is no question that the use of outsourced providers may be done ethically. The choice of whether to delegate work to an outsourced provider should be based on whether it allows a firm to help deliver outstanding and timely work to its clients.

Data security is not only a serious ethics concern when considering outsourcing legal services, it is also a central concern when it comes to working remotely during the COVID-19 pandemic. During this time it is imperative that law firms and companies institute cybersecurity measures to protect confidential and sensitive client and business information. All remote workers should be educated and aware of necessary cyber-hygiene measures, including ensuring a secure Wi-Fi connection, installing anti-virus software and encryption tools on home or laptop computers, locking the computer screen in a shared space, and backing up important files regularly. Juhan Lepassaar, executive director of the European Union Agency for CyberSecurity (ENISA) offers the following tips for employers:

- Communicate regularly with the workforce about potential problems and provide an emergency service;
- Provide remote access support solutions;
- Offer remote features such as electronic signatures and virtual workflows;
- Identify a clear procedure in the event of a security breach; and
- Restrict access to sensitive systems or information.

Much has been written about the surge in electronic data breaches at law firms. Most recently, Law.com reported there were over 5,000 data breaches at law firms in 2019. Many of these breaches are not the typical ransomware attack where a fee is sought to release blocked data. In February 2020, the hacking group behind a series of Maze ransomware attacks on several smaller and mid-size law firms steadily posted sensitive client data, personal client records, and confidential client information on the internet for public viewing. It is no longer a question of *if* your computer system will be hacked, but *when* will it happen.

The ABA's Model Rules of Professional Conduct provide that lawyers must take reasonable steps

to protect their client's data. Specifically, Rule 1.6(c), *Confidentiality of Information*, expressly provides: "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." The ABAs Standing Committee on Ethics and Professional Responsibility released Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*, on October 17, 2018, that reaffirms the lawyer's duty to notify clients of a data breach and details reasonable steps to take to meet obligations set forth by the ABA Model Rules. The opinion underscores the importance for lawyers to both plan for an electronic breach or cyberattack and to understand how the Model Rules come into play when an incident is either detected or suspected. ABA Formal Op. 483 states:

> Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Unfortunately, neither the Model Rules nor the ethics opinion explicitly address what constitutes "reasonable efforts." However, at a minimum, reasonable efforts to address data breach or cyberattack risks are twofold. First, reasonable efforts must include installing basic cybersecurity systems like anti-virus software, encryption, VPNs, firewalls, and the like on your firm's computer system. Second, and equally as important, reasonable efforts must include a hat trick of actions: comprehensive system assessment; cyber awareness training for employees, including proper email etiquette and how to avoid infected websites; and sporadic testing of employees. These actions are essential. Most law firm breaches are not the result of security systems that lack cybersecurity software. Indeed, most law firms are up to date in deploying technology to protect their data. However, the most common breaches are not caused by technological shortcomings, but instead are the result of user error.

Finally, law firms should conduct some simple and basic due diligence of its vendors who may be hosting their clients' data to ensure they have adequate security systems, training, and testing in place. As reported in Law360, legal services firm Epiq Global recently found malware on its network. Epiq's website states that it is:

> A worldwide provider of legal services, serving law firms, corporations, financial institutions and government agencies — helping them streamline the administration of business operations, class action and mass tort, court reporting, eDiscovery, regulatory, compliance, restructuring, and bankruptcy matters.

According to Law360, Epiq had to shut down its online services that prevented lawyers from accessing client data. Epiq indicated there was no unauthorized transfer of data by the malware. Law360 noted that this was not the first time a tech vendor in the legal industry was subjected to a hack. In October 2019, Trialworks was hit by a ransomware attack that prevented access to their data. In 2018, Digital Shadows reported that configuration errors had exposed 2.3 billion files to a security threat.

Ransomware has become a common form of attack against law firms. The best way to deal with malware is to prevent it from getting into your system in the first place. Make certain you keep your technology and your people up to date in order to protect your firm and your clients' data.