Reprinted with permission from: New York State Bar Association *Journal*, June/July 2020, Vol. 92, No. 5, published by the New York State Bar Association, One Elk Street, Albany, NY 12207.

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

TO THE FORUM:

I am the managing partner of a general practice law firm of approximately 40 lawyers and 20 staff members. In response to the ongoing pandemic, all firm employees are required to work from home. While the safety of the firm's employees is always a top priority, our management team has concerns about how our employees remain in compliance with their ethical obligations during this time. Specifically, with many of our attorneys working in close quarters to other family members, how can they best ensure they are safeguarding client's confidentiality?

Additionally, our firm has implemented a number of practices to facilitate a seamless transition when working from home. For example, we provide secure remote access protected with two-factor authentication for access to our work applications. We also provide a firm-hosted cloud-based file sharing service so that our employees can transfer multiple and high-volume files to clients as well as one another throughout the workday. Are there any specific ethical obligations we should be aware of with respect to the technology and working from home? How can our firm ensure that we are using technology safely, effectively and in compliance with our ethical obligations?

Separately and surprisingly, we have reached out to adversaries requesting extensions of deadlines, and one adversary in particular was obstinate refusing to give us an extension, despite the fact that my client was one of the many individuals who had become sick because of the pandemic, forcing us to make an application to the court. Is our adversary's conduct ethical? What principles of ethics should we adhere to when dealing with unreasonable adversaries?

Lastly, given that face-to-face communications are severely limited and individual accessibility is uncertain, what are our ethical obligations with respect to the supervision of subordinate attorneys and staff?

Sincerely,
Patty Partner

DEAR PATTY:

The global pandemic has undoubtedly forced us to steer a course through uncharted professional territory. It has created many professional and ethical challenges as lawyers have been compelled to practice law primarily in a remote work environment.

One of the most fundamental challenges that lawyers face when working from a remote location is the necessity to protect client confidences. As discussed in prior Forums, RPC 1.6 governs a lawyer's duty of confidentiality, and this duty applies in all settings and at all times.

When working at home, it is easy to adopt casual practices. Attorneys should be wary of falling into that trap. Working remotely often creates unique circumstances of having to work in close proximity to other family members. As a result, attorneys must take extra precautions to safeguard client confidences. For example, your "remote office" should be as autonomous as possible. It is best practice to avoid working in commonly used areas of your home such as the kitchen table or the living room.

However, we understand that this might not be feasible in every situation, especially for attorneys with younger children engaging in remote learning. If your circumstances do not permit you to create a designated and private workspace within your home, you should endeavor to set clear boundaries with children, partners and other members of your household as to how they should treat your workspace and work files. You also may want to consider investing in a locked filing cabinet to store sensitive information. If you do not have locked storage, we suggest that you store your work-related materials somewhere only you can access them. Attorneys should also consider practical efforts, such as not letting children or significant others access work devices for personal use and setting up a private, password-protected, Wi-Fi network specifically for your professional work. At a minimum, your work devices (laptops, tablets, phones) should always be password-protected with strong and unique passwords.

We also suggest that you do your best to become "tech-savvy" or competent in the technology you will need when working remotely. The NYSBA Committee on Professional Ethics (the "Committee") has opined that an attorney should only use technology that he or she is competent to use. See NYSBA Comm. on Prof'l Ethics, Op. 1025 (2014). Accordingly, a law firm should take appropriate steps to ensure that its attorneys are familiar with the firm's operating systems and computer programs and the firm's policies concerning the use of those systems/programs before transitioning to a fully remote work environment.

But, that is only half the battle. Attorneys also should be cognizant of the heightened risk of cybersecurity threats when working remotely. Comment [8] to RPC 1.1 states: "to maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." As addressed in a prior Forum, attorneys and law firms have an ethical obligation to institute and maintain sound cybersecurity protocol, and to ensure that third-party vendors do the same. See Vincent J. Syracuse, Maryann C. Stallone, Richard W. Trotter & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., June 2017, Vol. 89, No. 5.

Phishing scams are an example of a common cybersecurity threat to law firms. These scams include fraudulent emails that appear to be sent from a genuine source, such as a colleague, family member or personal banking institution, for the purpose of obtaining personal information, such as passwords and banking details, and defrauding attorneys or their firms. For this reason, attorneys should be extra vigilant when reviewing emails and downloading files. It is always a best practice to double check the email address of the sender and confirm the email is legitimate, as many hackers will create fake email accounts with only slight variations to that of the individual the hacker is purporting to impersonate. Attorneys also should avoid downloading files or clicking on links from an email that they are not expecting, and immediately bring emails that appear to be suspicious to the attention of the firm's IT department for further investigation.

Furthermore, we recommend that attorneys access their firm networks remotely through a Virtual Private Network (VPN), an encrypted connection over the internet from a device to a network. The encrypted connection

helps ensure that sensitive data is safely transmitted over the internet. Firms should always keep their VPNs current and deploy all patches with updated security configurations. Moreover, it is critical to maintain proper multi-factor authentication for all VPN access to networks.

Cybersecurity threats also arise with the use of cloud-based file-sharing services to send and receive confidential client documents. A 2014 report by the Department of Homeland Security recognized that "online tools that help millions of Americans work from home may be exposing both workers and businesses to cybersecurity risks." Michael Roppolo, Work-from-home remote access software vulnerable to hackers: Report, CBS News (July 31, 2014).

In two ethics opinions issued in 2014, the Committee concluded that giving lawyers remote access to client files was not unethical, as long as the technology used provides reasonable protection to confidential client information, or the law firm informs the client of the risks and obtains informed consent from the client to proceed. See NYSBA Comm. on Prof'l Ethics, Op. 1019 (2014) and NYSBA Comm. on Prof'l Ethics, Op. 1020 (2014). In Opinion 1019, the Committee noted that "because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients." Id. However, Comment [17] to RPC 1.6 instructs us that "[t]he key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure." RPC 1.6, Comment [17].

To meet the reasonable care standard set forth in RPC 1.6, attorneys should consult with their firm's IT department or service provider to investigate whether their firm's file-sharing services implement reasonable security measures to protect client confidence. Where possible, the firm should implement two-factor authentication to access its work applications and software. If after speaking with your IT provider/personnel you continue to have doubts as to security, you should obtain the client's consent before sharing any files or documents. The failure to employ basic data-security measures can have severe consequences, including civil liability for professional malpractice.

A security measure that law firms should consider implementing to protect client confidences is the encryption of files and emails sent both inside and outside the firm. Encryption is the process of converting digital information into a code, to prevent unauthorized access by outside parties

Additional best practices in addressing cybersecurity risks include: (1) understanding and using reasonable security measures, such as secure internet access methods; when accessing files remotely, attorneys should avoid logging on to unsecured Wi-Fi networks or "hotspots," which can expose both the attorney and the firm's files to malware – software designed by hackers that can infiltrate remote desktops and whose capabilities include logging keystrokes, uploading discovered data, updating malware and executing further malware; (2) training non-lawyer support staff in the handling of confidential client information and to report suspicious activity; (3) clearly and conspicuously labelling confidential client information as "privileged and confidential"; (4) conducting due diligence on third-party vendors providing digital storage and communication technology; (5) creating and implementing a data breach incident response plan; and (6) assessing the need for cyber insurance for data breaches. See ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 477 (May 2017).

Using secure internet access is of critical importance to avoid a man-in-the-middle attack, or "MITM" attack, which occurs when the communication between two systems is intercepted by a third party, i.e., a Man-in-the-Middle. This can happen in any form of online communication, such as email, web-browsing, and even social media. The MITM can use a public Wi-Fi connection to gain access to your browser, or even compromise your entire device. Once the MITN gains access to your device they have the ability to steal your credentials, transfer data files, install malware, or even spy on the user. To avoid the potentially significant and disastrous effects of a MITM attack, you should work off a secure Wi-Fi network and avoid using "hotspots."

Additionally, when using video-conferencing platforms such as Zoom, make sure that your meetings are password-protected to avoid a type of cyberattack called "Zoom-bombing," where strangers hijack a private Zoom teleconferencing chat and draw offensive imagery onscreen, such as pornographic images, personal information of the individuals in the chat, and even taunting them with hate speech and threats.

Turning to the part of your question regarding the civility (or lack thereof) of your adversary, the pandemic is certainly no excuse for bad behavior. As discussed in a recent Forum, RPC 3.4 governs "fairness to opposing party and counsel" and provides that when dealing with an opposing party and the opposing party's counsel, an attorney must act with fairness and candor. See RPC 3.4; see also Vincent J. Syracuse, Maryann C. Stallone, Carl F. Regelmann & Alyssa C. Goldrich, Attorney Professionalism Forum, N.Y. St. B.J., April 2020, Vol. 92, No. 3. The commentary to Rule 1.2 further provides that in

accomplishing the client's objectives, the lawyer should not be offensive, discourteous, inconsiderate or dilatory. RPC 1.2 Comment [16]. And, while the RPC does not specifically address an attorney adversary's obligations under Rule 3.4 or 1.2 in the wake of a global pandemic, it is axiomatic that lawyers should be particularly sensitive to reasonable requests for extensions under such circumstances.

While your adversary's refusal to grant you a reasonable extension is not a per se violation of the RPC or a basis for a report to the Disciplinary Committee, such conduct may violate the New York State Standards of Civility (the "Standards"), particularly if this is the first time you are asking for an extension on the motion. See 22 N.Y.C.R.R. § 1200, App. A. As discussed in a prior Forum, the Standards of Civility were adopted as a guide for the legal profession, including lawyers, judges and court personnel, and outline basic principles of behavior to which lawyers should aspire. See Vincent J. Syracuse, Maryann C. Stallone & Hannah Furst, Attorney Professionalism Forum, N.Y. St. B.J., March/April 2016, Vol. 88, No. 3.

The language of the Standards of Civility is clear – in the absence of a court order, a lawyer should agree to reasonable requests for extensions of time when the legitimate interests of the client will not be adversely affected. See 22 N.Y.C.R.R. § 1200, App. A. An adversary who refuses to provide a reasonable extension during the global pandemic in order to gain some tactical advantage is not just exhibiting bad form, but is creating a negative reputation and relationship with their adversary that may ultimately adversely affect their position in the litigation. By way of example, an uncooperative attorney is unlikely to get a professional courtesy in the future. Moreover, judges and juries generally do not look kindly upon attorneys that do not extend professional courtesies. In the ordinary course, reasonable requests for extensions of time should be handled by the attorneys in the case, not by the courts.

The flip side to this scenario, which is also likely to occur, is attorneys using the pandemic as an excuse for their dilatory tactics to delay the case and frustrate your client's ability to recover. As is the case with many ethical rules, the deciding factor in whether to grant or deny a request for an extension is the reasonableness of the request.

Separately, your obligations with respect to the supervision of subordinate attorneys remain unchanged. RPC 5.1 sets forth the responsibilities of law firms, partners, and managers over other lawyers. Lawyers serving in a managerial or supervisory role are required to make reasonable efforts to ensure that all attorneys comply with their ethical obligations. This duty becomes even more important in a time of disaster or emergency. See RPC 5.1. Specifically, RPC 5.1(b) requires lawyers with management or direct supervisory authority over other lawyers in the firm to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the RPC such as identifying dates by which actions must be taken in pending matters and ensuring that inexperienced lawyers are appropriately supervised. See RPC 5.1, Comment [2].

There are no bright line rules governing supervision. Comment [3] to RPC 5.1 tells us that each law firm should carefully consider the structure and nature of its practice when adopting policies governing the supervision of subordinate attorneys. See RPC 5.1, Comment [3]. For example, if the firm is relatively small and consists of mostly experienced lawyers, informal supervision and periodic review of compliance with the required policies will ordinarily suffice. Conversely, if the firm is much larger, and employs numerous junior attorneys, more elaborate measures may be necessary to place the firm in compliance with RPC 5.1. Id.

The degree of supervision required also varies on a case-by-case basis and is generally judged by what is reasonable under the circumstances. Factors that should be considered include: (i) the experience of the person whose work is being supervised, (ii) the amount of work involved in a particular matter, and (iii) the likelihood that ethical problems might arise while working on the matter. See id.

Generally speaking, it is best practice for supervising attorneys to remain apprised of subordinate attorneys' workload, implement a system for review of the subordinate attorney's work product and ensure that the subordinate attorney understands that system. In our experience, requiring subordinate attorneys to submit weekly status reports detailing the matters they are working on is a good first step to guarantee that no matter falls through the cracks.

Supervising attorneys also should establish an open line of communication with subordinate attorneys. In today's age, there are many mediums that allow for regular communication in this remote work environment, including video conferencing (via Zoom or Skype), telephone calls, email and even text messages. Therefore, in addition to communicating via email, a supervising attorney should schedule regular calls (via Zoom, Skype or telephone) with subordinate attorneys to check on their progress and review and discuss their work product and workload. How often you communicate with the individuals under your supervision will depend on the complexity of the matter and issues, and the upcoming deadlines in those matters. This too is a matter of the lawyer's reasonable judgment and care.

Notably, RPC 5.1(d) articulates a general principle of personal responsibility for acts of other lawyers in the law firm and imposes such responsibility on a lawyer who orders, directs or ratifies wrongful conduct and on lawyers who are partners or who have comparable managerial authority in a law firm who know or reasonably should know of the conduct. See RPC 5.1(d). Thus, lawyers acting in a supervisory or managerial role should be aware that their failure to exercise diligence in reviewing the work of subordinate attorneys may result in personal liability under RPC 5.1(d).

Whether you are working in the office or remotely, attorneys should always use their best efforts so that client communication and diligent representation continues uninterrupted. One of our prior Forums referred attorneys to RPC 1.4, which governs an attorney's obligations with respect to communicating with clients. RPC 1.4 states that attorneys are ethically obligated to promptly comply with reasonable requests for information from clients. RPC 1.4(a)(4); see Vincent J. Syracuse, Maryann C. Stallone & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., July/August 2016, Vol. 88, No. 6. To avoid noncompliance with RPC 1.4 while working remotely, attorneys should inform clients of the best way to reach them. If, for example, an attorney is able to forward calls from the office line to a personal cell phone, the attorney can tell clients that they may still use the office number. If attorneys do not have this ability, they need to advise their clients what alternate number they can be reached at (whether a cell phone number or home landline). In addition, attorneys should regularly check their office voicemail and email and avoid large gaps in response time.

Finally, attorneys must continue to maintain their professionalism and decorum despite working from the comfort of their homes. We have previously talked about the importance of dressing appropriately when appearing in front of a tribunal; proper dress is part of basic professionalism and a sign of respect. See Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. St. B.J., May 204, Vol. 86, No. 4. That standard still applies when participating in a virtual court conference, as well as video arbitrations and mediations. Judge Dennis Bailey of Broward County Florida recently expressed his dismay that attorneys appeared inappropriately on camera for virtual court hearings: "It is remarkable how many attorneys appear inappropriately on camera," Bailey said. "We've seen many lawyers in casual shirts and blouses, with no concern for ill-grooming, in bedrooms with the master bed in the background, etc. One male lawyer appeared shirtless and one female attorney appeared still in bed, still under the covers. And putting on a beach cover-up won't cover up that you're poolside in a bathing suit. So, please, if you don't mind, let's treat court hearings as court hearings, whether Zooming or not." Debra Cassens Weiss, Lawyers are dressing way too casual during Zoom court hearings, judge says, ABA Journal (Apr. 15, 2020), https://www.abajournal.com/news/article/lawyers-are-dressing-way-too-casual-during-zoom-hearings-judge-says.

As always, the devil is in the details. What is deemed appropriate can be subjective, and there may not always be agreement on what should be worn when in a virtual court or ADR proceeding. Certainly, going shirtless, wearing a bathing suit or video conferencing from your bed is never appropriate. You should use common sense, and when in doubt, it is best to err on the side of caution and overdress to avoid facing the risk of having your choice of clothing overshadow the needs of your client or what you might be saying.

Sincerely,
The Forum by
Vincent J. Syracuse, Esq.
(syracuse@thsh.com)
Maryann C. Stallone, Esq.
(stallone@thsh.com) and
Alyssa C. Goldrich, Esq.
(goldrich@thsh.com)
Tannenbaum Helpern Syracuse & Hirschtritt LLP

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

DEAR FORUM:

I am an attorney in private practice focusing on personal injury law here in New York. I also do a bit of matrimonial law. My clients come from underserved communities, and many face extreme financial hardships. I've always known that Rule 1.8(e) prohibits giving financial assistance to clients in connection with a pending litigation and, as much as I have wanted to, I never gave anyone a dime. Rather, over the years, I developed a nice Rolodex with contacts at public service associations to refer these clients to so they could get their needs met. But with all this Covid-19 stuff going on it has gotten way worse and so many have now found themselves without a paycheck and are simply unable to meet their day-to-day needs. The public service organizations have been inundated, and my clients are unable to get desperately needed help. I was recently approached by a client, a young parent of two preschool-aged children, who is unable to buy groceries. And while I know that I probably shouldn't have, I figured that it would be okay to give him a few bucks for a couple of bags of groceries. He's a good kid and I know the money is going to his children. I am concerned I may have done something wrong but it really was so little to me and so much to him. What should I have done?

Sincerely,
Justa Bene Mensch