

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 498

March 10, 2021

Virtual Practice

The ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm.¹ When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.

I. Introduction

As lawyers increasingly use technology to practice virtually, they must remain cognizant of their ethical responsibilities. While the ABA Model Rules of Professional Conduct permit virtual practice, the Rules provide some minimum requirements and some of the Comments suggest best practices for virtual practice, particularly in the areas of competence, confidentiality, and supervision. These requirements and best practices are discussed in this opinion, although this opinion does not address every ethical issue arising in the virtual practice context.²

II. Virtual Practice: Commonly Implicated Model Rules

This opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional brick-and-mortar law firm.³ A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

² Interstate virtual practice, for instance, also implicates Model Rule of Professional Conduct 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law, which is not addressed by this opinion. See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 495 (2020), stating that "[l]awyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction."

³ See generally MODEL RULES OF PROFESSIONAL CONDUCT R. 1.0(c), defining a "firm" or "law firm" to be "a lawyer or lawyers in a partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization on the legal department of a corporation or other organization." Further guidance on what constitutes a firm is provided in Comments [2], [3], and [4] to Rule 1.0.

have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need. Although the ethics rules apply to both traditional and virtual law practice,⁴ virtual practice commonly implicates the key ethics rules discussed below.

A. *Commonly Implicated Model Rules of Professional Conduct*

1. Competence, Diligence, and Communication

Model Rules 1.1, 1.3, and 1.4 address lawyers' core ethical duties of competence, diligence, and communication with their clients. Comment [8] to Model Rule 1.1 explains, "To maintain the requisite knowledge and skill [to be competent], a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (*Emphasis added*). Comment [1] to Rule 1.3 makes clear that lawyers must also "pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor." Whether interacting face-to-face or through technology, lawyers must "reasonably consult with the client about the means by which the client's objectives are to be accomplished; . . . keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information. . . ." ⁵ Thus, lawyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually.⁶

2. Confidentiality

Under Rule 1.6 lawyers also have a duty of confidentiality to all clients and therefore "shall not reveal information relating to the representation of a client" (absent a specific exception, informed consent, or implied authorization). A necessary corollary of this duty is that lawyers must at least "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."⁷ The following non-

⁴ For example, if a jurisdiction prohibits substantive communications with certain witnesses during court-related proceedings, a lawyer may not engage in such communications either face-to-face or virtually (e.g., during a trial or deposition conducted via videoconferencing). *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 3.4(c) (prohibiting lawyers from violating court rules and making no exception to the rule for virtual proceedings). Likewise, lying or stealing is no more appropriate online than it is face-to-face. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.15; MODEL RULES OF PROF'L CONDUCT R. 8.4(b)-(c).

⁵ MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(2) – (4).

⁶ Lawyers unexpectedly thrust into practicing virtually must have a business continuation plan to keep clients apprised of their matters and to keep moving those matters forward competently and diligently. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) (discussing ethical obligations related to disasters). Though virtual practice is common, if for any reason a lawyer cannot fulfill the lawyer's duties of competence, diligence, and other ethical duties to a client, the lawyer must withdraw from the matter. MODEL RULES OF PROF'L CONDUCT R. 1.16. During and following the termination or withdrawal process, the "lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred." MODEL RULES OF PROF'L CONDUCT R. 1.16(d).

⁷ MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

exhaustive list of factors may guide the lawyer’s determination of reasonable efforts to safeguard confidential information: “the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”⁸ As ABA Formal Op. 477R notes, lawyers must employ a “fact-based analysis” to these “nonexclusive factors to guide lawyers in making a ‘reasonable efforts’ determination.”

Similarly, lawyers must take reasonable precautions when transmitting communications that contain information related to a client’s representation.⁹ At all times, but especially when practicing virtually, lawyers must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information. This responsibility “does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.”¹⁰ However, depending on the circumstances, lawyers may need to take special precautions.¹¹ Factors to consider to assist the lawyer in determining the reasonableness of the “expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.”¹² As ABA Formal Op. 477R summarizes, “[a] lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access.”

3. Supervision

Lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct.¹³ Practicing virtually does not change or diminish this obligation. “A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product.”¹⁴ Moreover, a lawyer must “act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent

⁸ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18].

⁹ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [19].

¹⁰ *Id.*

¹¹ The opinion cautions, however, that “a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.” ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

¹² MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [19].

¹³ MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3. *See, e.g.*, ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 467 (2014) (discussing managerial and supervisory obligations in the context of prosecutorial offices). *See also* ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 n.6 (2018) (describing the organizational structures of firms as pertaining to supervision).

¹⁴ MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [2].

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.*"¹⁵ The duty to supervise nonlawyers extends to those both within and outside of the law firm.¹⁶

B. *Particular Virtual Practice Technologies and Considerations*

Guided by the rules highlighted above, lawyers practicing virtually need to assess whether their technology, other assistance, and work environment are consistent with their ethical obligations. In light of current technological options, certain available protections and considerations apply to a wide array of devices and services. As ABA Formal Op. 477R noted, a "lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software." Furthermore, "[o]ther available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems." To apply and expand on these protections and considerations, we address some common virtual practice issues below.

1. Hard/Software Systems

Lawyers should ensure that they have carefully reviewed the terms of service applicable to their hardware devices and software systems to assess whether confidentiality is protected.¹⁷ To protect confidential information from unauthorized access, lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs). Finally, as technology inevitably evolves, lawyers should periodically assess whether their existing systems are adequate to protect confidential information.

¹⁵ MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (emphasis added).

¹⁶ As noted in Comment [3] to Model Rule 5.3:

When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law).

¹⁷ For example, terms and conditions of service may include provisions for data-soaking software systems that collect, track, and use information. Such systems might purport to own the information, reserve the right to sell or transfer the information to third parties, or otherwise use the information contrary to lawyers' duty of confidentiality.

2. Accessing Client Files and Data

Lawyers practicing virtually (even on short notice) must have reliable access to client contact information and client records. If the access to such “files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer.”¹⁸ Lawyers must ensure that data is regularly backed up and that secure access to the backup data is readily available in the event of a data loss. In anticipation of data being lost or hacked, lawyers should have a data breach policy and a plan to communicate losses or breaches to the impacted clients.¹⁹

3. Virtual meeting platforms and videoconferencing

Lawyers should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer’s ethical obligations. Access to accounts and meetings should be only through strong passwords, and the lawyer should explore whether the platform offers higher tiers of security for businesses/enterprises (over the free or consumer platform variants). Likewise, any recordings or transcripts should be secured. If the platform will be recording conversations with the client, it is inadvisable to do so without client consent, but lawyers should consult the professional conduct rules, ethics opinions, and laws of the applicable jurisdiction.²⁰ Lastly, any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by other third parties who are not assisting with the representation,²¹ to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality.

4. Virtual Document and Data Exchange Platforms

In addition to the protocols noted above (e.g., reviewing the terms of service and any updates to those terms), lawyers’ virtual document and data exchange platforms should ensure that

¹⁸ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 482 (2018).

¹⁹ See, e.g., ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 (2018) (“Even lawyers who, (i) under Model Rule 1.6(c), make ‘reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,’ (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients ‘reasonably informed’ and with an explanation ‘to the extent necessary to permit the client to make informed decisions regarding the representation.’”).

²⁰ See, e.g., ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 01-422 (2001).

²¹ Pennsylvania recently highlighted the following best practices for videoconferencing security:

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to “Host Only;”
- Ensure users are using the updated version of remote access/meeting applications.

Pennsylvania Bar Ass’n Comm. on Legal Ethics & Prof’l Responsibility, Formal Op. 2020-300 (2020) (citing an FBI press release warning of teleconference and online classroom hacking).

documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure. For example, if the lawyer is transmitting information over email, the lawyer should consider whether the information is and needs to be encrypted (both in transit and in storage).²²

5. Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices

Unless the technology is assisting the lawyer's law practice, the lawyer should disable the listening capability of devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters. Otherwise, the lawyer is exposing the client's and other sensitive information to unnecessary and unauthorized third parties and increasing the risk of hacking.

6. Supervision

The virtually practicing managerial lawyer must adopt and tailor policies and practices to ensure that all members of the firm and any internal or external assistants operate in accordance with the lawyer's ethical obligations of supervision.²³ Comment [2] to Model Rule 5.1 notes that "[s]uch policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

a. Subordinates/Assistants

The lawyer must ensure that law firm tasks are being completed in a timely, competent, and secure manner.²⁴ This duty requires regular interaction and communication with, for example,

²² See, e.g., ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) (noting that "it is not always reasonable to rely on the use of unencrypted email").

²³ As ABA Formal Op. 477R noted:

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

²⁴ The New York County Lawyers Association Ethics Committee recently described some aspects to include in the firm's practices and policies:

- Monitoring appropriate use of firm networks for work purposes.
- Tightening off-site work procedures to ensure that the increase in worksites does not similarly increase the entry points for a data breach.
- Monitoring adherence to firm cybersecurity procedures (e.g., not processing or transmitting work across insecure networks, and appropriate storage of client data and work product).
- Ensuring that working at home has not significantly increased the likelihood of an inadvertent disclosure through misdirection of a transmission, possibly because the lawyer or nonlawyer was distracted by a child, spouse, parent or someone working on repair or maintenance of the home.

associates, legal assistants, and paralegals. Routine communication and other interaction are also advisable to discern the health and wellness of the lawyer's team members.²⁵

One particularly important subject to supervise is the firm's bring-your-own-device (BYOD) policy. If lawyers or nonlawyer assistants will be using their own devices to access, transmit, or store client-related information, the policy must ensure that security is tight (e.g., strong passwords to the device and to any routers, access through VPN, updates installed, training on phishing attempts), that any lost or stolen device may be remotely wiped, that client-related information cannot be accessed by, for example, staff members' family or others, and that client-related information will be adequately and safely archived and available for later retrieval.²⁶

Similarly, all client-related information, such as files or documents, must not be visible to others by, for example, implementing a "clean desk" (and "clean screen") policy to secure documents and data when not in use. As noted above in the discussion of videoconferencing, client-related information also should not be visible or audible to others when the lawyer or nonlawyer is on a videoconference or call. In sum, all law firm employees and lawyers who have access to client information must receive appropriate oversight and training on the ethical obligations to maintain the confidentiality of such information, including when working virtually.

b. Vendors and Other Assistance

Lawyers will understandably want and may need to rely on information technology professionals, outside support staff (e.g., administrative assistants, paralegals, investigators), and vendors. The lawyer must ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties. When appropriate, lawyers should consider use of a confidentiality agreement,²⁷ and should ensure that all client-related information is secure, indexed, and readily retrievable.

7. Possible Limitations of Virtual Practice

Virtual practice and technology have limits. For example, lawyers practicing virtually must make sure that trust accounting rules, which vary significantly across states, are followed.²⁸ The

-
- Ensuring that sufficiently frequent "live" remote sessions occur between supervising attorneys and supervised attorneys to achieve effective supervision as described in [New York Rule of Professional Conduct] 5.1(c).

N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 754-2020 (2020).

²⁵ See ABA MODEL REGULATORY OBJECTIVES FOR THE PROVISION OF LEGAL SERVICES para. I (2016).

²⁶ For example, a lawyer has an obligation to return the client's file when the client requests or when the representation ends. See, e.g., MODEL RULES OF PROF'L CONDUCT R. 1.16(d). This important obligation cannot be fully discharged if important documents and data are located in staff members' personal computers or houses and are not indexed or readily retrievable by the lawyer.

²⁷ See, e.g., Mo. Bar Informal Advisory Op. 20070008 & 20050068.

²⁸ See MODEL RULES OF PROF'L CONDUCT R. 1.15; See, e.g., ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) ("Lawyers also must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust. A lawyer's obligations with respect to these funds will vary depending on the circumstances. Even before a disaster, all lawyers should consider (i) providing for another trusted signatory on trust

lawyer must still be able, to the extent the circumstances require, to write and deposit checks, make electronic transfers, and maintain full trust-accounting records while practicing virtually. Likewise, even in otherwise virtual practices, lawyers still need to make and maintain a plan to process the paper mail, to docket correspondence and communications, and to direct or redirect clients, prospective clients, or other important individuals who might attempt to contact the lawyer at the lawyer's current or previous brick-and-mortar office. If a lawyer will not be available at a physical office address, there should be signage (and/or online instructions) that the lawyer is available by appointment only and/or that the posted address is for mail deliveries only. Finally, although e-filing systems have lessened this concern, litigators must still be able to file and receive pleadings and other court documents.

III. Conclusion

The ABA Model Rules of Professional Conduct permit lawyers to conduct practice virtually, but those doing so must fully consider and comply with their applicable ethical responsibilities, including technological competence, diligence, communication, confidentiality, and supervision.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Lynda Shely, Scottsdale, AZ ■ Melinda Bentley, Jefferson City, MO ■ Lonnie T. Brown, Athens, GA ■ Doug Ende, Seattle, WA ■ Robert Hirshon, Ann Arbor, MI ■ David M. Majchrzak, San Diego, CA ■ Thomas B. Mason, Washington, D.C. ■ Norman W. Spaulding, Stanford, CA ■ Keith Swisher, Scottsdale, AZ ■ Lisa D. Taylor, Parsippany, NJ

CENTER FOR PROFESSIONAL RESPONSIBILITY: Mary McDermott, Senior Counsel

©2021 by the American Bar Association. All rights reserved.

accounts in the event of the lawyer's unexpected death, incapacity, or prolonged unavailability and (ii) depending on the circumstances and jurisdiction, designating a successor lawyer to wind up the lawyer's practice.”).