149

Ethical Obligations for Lawyers Engaging in Virtual Practice

I. Introduction and Scope

The COVID-19 pandemic resulted in many lawyers adopting alternative methods of providing legal services, including incorporating virtual procedures into their practices. While the pandemic has ended, the pandemic fundamentally changed how the legal community views virtual practice options. The legal community continues to provide services in hybrid environments (both the physical office and remotely) and even completely virtually.[1] This opinion addresses the Colorado Rules of Professional Conduct (Colo. RPC or Rules) that lawyers should consider when engaging in any type of virtual law practice.

II. Syllabus

The American Bar Association (ABA) broadly defines a virtual law practice as a "technically enabled law practice beyond the traditional brick-and-mortar firm."[2] The absence of a traditional physical law office can create new issues with respect to certain ethical rules that a lawyer in a traditional setting may not confront. These rules include Rule 1.1 (competence), Rule 1.3 (diligence), Rule 1.4 (communication), Rule 1.6

---

[1] This Opinion uses the terms "virtual practice" and "remote practice" synonymously.

[2] ABA Comm. on Ethics and Prof. Resp., Formal Op. 498, "Virtual Practice" (2021), p. 1 (ABA Opinion 498).

(confidentiality), Rules 5.1 and 5.3 (proper supervision), and Rule 5.5 (unauthorized practice of law).

Since the pandemic, the ABA has published two opinions addressing the model versions of these rules and how they apply to virtual practice. *See* ABA Comm. on Ethics and Prof. Resp., Formal Op. 495, ABA Opinion 498. ABA Opinion 495 focuses on guidance for attorneys practicing remotely from jurisdictions in which they are not licensed and associated potential pitfalls. ABA Opinion 498 gives more general guidance to lawyers and law firms practicing virtually and discusses best practices for complying with the ABA Model Rules of Professional Conduct.

This opinion compares the Colo. Rules with these ABA opinions and the opinions of other jurisdictions to provide guidance for Colorado lawyers practicing law in virtual and hybrid environments.

III. Analysis

A. Rule 1.1 (Competence)

Under the Colo. RPC, a lawyer has a duty of competence. Colo. RPC 1.1 states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

The duty of competence requires a lawyer not only have expertise in their practice area, but also, generally, in the technology needed to practice law and rules regarding the use of technology in their practice.[3] Although Colo. RPC 1.1 itself is silent on technological

[3] *See, e.g.*, Chief Justice Directive 23-03 (regarding virtual proceedings policy); 2023 COLO. SESS. LAWS, Ch. 415 (regarding remote participation in residential evictions).

expertise, comment [8] to the rule explains that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and *changes in communications and other relevant technologies*, [and] engage in continuing study and education…." Colo. RPC 1.1, cmt [8] (emphasis added).

According to ABA Opinion 498, ABA Model Rule 1.1 takes the competency requirement regarding technology one step further. In 2012, the ABA modified comment [8] to ABA Model Rule 1.1. Similar, in part, to Colorado's RPC 1.1, ABA Model Rule 1.1 cmt. [8] states that "[t]o 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*, [and] engage in continuing study and education…." ABA Model Rule 1.1, cmt. [8] (emphasis added).

The Wisconsin Ethics Commission also has addressed virtual practice. It cited Comment [8] to ABA Model Rule 1.1 as defining basic technological competence to include, at a minimum, "knowledge of the types of devices available for communication, software options for communication, preparation, transmission and storage of documents and other information, and the means to keep the devices and the information they transmit and store secure and private." Wisc. Prof. Ethics Comm., Formal Ethics Opinion EF-21-02, "Working remotely," p. 2 (Jan. 29, 2021) (Wisconsin Opinion 21-02).

Unlike ABA Model Rule 1.1 cmt. [8], Colo. RPC 1.1 cmt. [8] does not include a reference to assessing the benefits and risks of technology. the practical application of this distinction has not been litigated in Colorado, however, and Colo. RPC 1.1 cmt. [8] makes specific reference to staying aware of changes in "communications and other relevant

technologies." This Committee therefore recommends Colorado lawyers follow the best practices discussed in Section IV below.

B. Rule 1.3 (Diligence)

Colo. RPC 1.3 requires lawyers to act with reasonable diligence and promptness when representing a client. Colo. RPC 1.3 cmt. [1] gives substance to the duty of diligence by stating that "[a] lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer…."[4] ABA Opinion 498 interpreted ABA Model Rule 1.3' analog to this comment, explaining that lawyers *must* "pursue a matter on behalf of a client despite opposition, obstruction[,] or personal inconvenience to the lawyer." ABA Opinion 498, p. 2. Opinion 498 suggests that ABA Model Rule 1.3 cmt. [1]means that a lawyer is held to the same core diligence standards regardless of any unique or additional challenges that a lawyer might encounter when practicing virtually.

Wisconsin also addresses the duty of diligence in the context of virtual practice and the unique challenges it presents. Wisconsin's opinion emphasizes that the duty requires reasonable diligence, "which implies that particular circumstances may affect the parameters of this duty." Wisconsin Opinion 21-02, p. 3. In the context of practicing remotely, difficulties with providing diligent representation can be avoided if a firm has systems in place to access files, conduct research in a timely fashion, and facilitate collaboration with others, notwithstanding a lawyer's non-physical presence.

Wisconsin's opinion also mentions that included within the duty of diligence is the

[4] ABA Model Rule 1.3 cmt. [1] and Colo. RPC 1.3 cmt. [1] are identical.

issue of contingency and succession planning. Wisconsin Opinion 21-02, p. 3. The opinion goes so far to say that "[d]evelopment of a succession plan is part of the lawyer's duty to provide competent and diligent representation." *Id.* For solo practitioners, the opinion directs lawyers to reach out to other lawyers to develop a plan to protect clients in the event of the lawyer's impairment. *Id.* In the firm context, management should plan for other members of the firm to become responsible for the unavailable lawyer's cases. *Id.* In support of its position, the Wisconsin opinion references ABA Model Rule 1.3, cmt. [5], which states:

> To prevent neglect of client matters in the event of a sole practitioner's death or disability, the duty of diligence may require that each sole practitioner prepare a plan, in conformity with applicable rules, that designates another competent lawyer to review client files, notify each client of the lawyer's death or disability, and determine whether there is a need for immediate protective action.

Id.

Colo. RPC 1.3 cmt. [5] is identical to the ABA Model Rule. This comment, however, only *suggests* that due diligence includes the development of a succession plan. Although not required by Colo. RPC 1.3 expressly, succession planning should be a vital consideration when a lawyer is practicing virtually.[5] The lawyer's physical separation from others heightens the risk that others may be unaware when a lawyer unexpectedly becomes incapacitated or dies. The Committee, therefore, urges lawyers with virtual practices, and solo practitioners in particular, to safeguard their clients' interests by creating a

[5] *See* CBA Formal Op. 147, "Expecting the Unexpected: Ethical Considerations in Succession Planning" (Jan. 18, 2024) (providing guidance and discussing ethical considerations when developing a succession plan).

contingency or succession plan as a best practice, even though it is not a technical requirement of the duty of diligence.

C. Rule 1.4 (Communication)

Colo. RPC 1.4 requires a lawyer to "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…." Colo. RPC 1.4(a)(2)–(4). ABA Opinion 498 concludes that nothing in ABA Model Rule 1.4[6] limits these obligations to face-to-face interactions. This Committee agrees. Communication when working virtually includes a variety of media – such as telephone, email, video conferencing, and texting – often eliminating any in-person interactions with clients. A lawyer therefore needs to ensure that a potential client is able to utilize the different media or the lawyer will be unable to inform and consult with the client as required.

Similarly, an opinion issued by the Virginia Standing Committee on Legal Ethics regarding virtual law practices states that "although the method of communication does not affect the lawyer's duty to communicate with the client, if the communication will be conducted primarily or entirely electronically, the lawyer may need to take extra precautions to ensure that communication is adequate and that it is received and understood by the client." VA Legal Ethics Op 1872, "Virtual Law Office and Use of Executive Office Suites" (Oct. 2, 2019), p. 1 (Virginia Opinion 1872). In a previous ethics opinion, Virginia

[6] ABA Model Rule 1.4 and Colo. RPC 1.4 are identical.

State Bar's Standing Committee on Legal Ethics concluded that a lawyer could permissibly represent clients with whom the lawyer had no in-person contact because "Rule 1.4 in no way dictates whether the lawyer should provide that information in a meeting, in writing, in a phone call, or in any particular form of communication. In determining whether a particular attorney has met this obligation with respect to a particular client, what is critical is *what* information was transmitted, not *how*." VA Legal Ethics Op. 1791, "Is It Ethical Not To Meet Face-to-Face With Your Client If You Communicate By E-mail or Telephone Instead" (Dec. 22, 2003), p. 2.

Virginia nevertheless cautioned that Rule 1.4(b) also requires that "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Virginia Opinion 1872, p. 2. To "explain" a matter implies a lawyer must take steps beyond merely providing information to ensure that a client is actually in a position to make informed decisions. *Id.* For example, a lawyer cannot simply upload information on a client portal and assume that their duty of communication is fulfilled without some confirmation from the client that they have received and understood the information provided. *Id.*

The Committee agrees that a lawyer should ensure that a client communication is received and understood, regardless of the method of transmittal. It is important to note that whether confirmation from the client that the virtual information has been sufficiently received and understood may depend on the facts of the situation, such as the sophistication of the client or the complexity of the information being conveyed. This obligation therefore may require that the lawyer follow-up with the client to discuss the information provided

and to answer any questions, whether the follow-up is in writing, by telephone, or even in person.

D. Rule 1.6 (Confidentiality)

The duty of confidentiality under Colo. RPC 1.6 prohibits lawyers from revealing information relating to the representation of a client, unless specific circumstances apply. As part of this duty, Colo. RPC 1.6(c) specifies that a lawyer must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." According to ABA Opinion 498, this means that lawyers, especially when practicing virtually, must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information. ABA Opinion 498, p. 3. Reasonable methods may vary across platforms or storage devices.

Comment [18] to Colo. RPC 1.6 provides a non-exhaustive list of factors to help a lawyer determine whether the efforts to safeguard confidential information are reasonable. Factors in determining reasonableness include, but are not limited to, "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)." Colo. RPC 1.6 cmt. [18]. ABA Opinion 498 adds that "lawyers must employ a 'fact-based analysis' to these 'nonexclusive factors to guide lawyers in making a reasonable efforts determination.'" ABA Opinion 498, p.3 (citing ABA Comm. on Ethics and Prof. Resp.

Formal Op. 477R, "Securing Communication of Protected Client Information" (revised May 22, 2017) (ABA Opinion 477R).

Rule 1.6's comments explain that the responsibility to prevent client information from ending up in the hands of unintended recipients "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy." Colo. RPC 1.6 cmt. [19]. Special circumstances, however, may warrant special precautions, taking into consideration factors such as "the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement." *Id.*

ABA Opinion 498 reiterates that transmitting information protected under Rule 1.6(a) is generally permissible where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. The ABA's position relies on the ABA Opinion 477R, which states "[t]he Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection." ABA Opinion 477R, p. 2. Opinion 477R explained that the ABA's adoption of Model Rule 1.6(c) and Comments [18] and [19] does not require specific security steps in all cases. *Id.* It also does not suggest that any breach in security is an automatic rule violation. The rule requires lawyers only to take "reasonable efforts" to secure client information. *Id.*

Virtual practice along with virtual communications therefore requires a fact-specific analysis to determine "reasonable efforts." As noted in Wisconsin's opinion, "[p]erhaps

no professional obligation has been impacted more by technology than the duty of confidentiality." Wisconsin Opinion 21-02, pp. 3-4. Although the use of technology has increased convenience, it also has increased the risk of inadvertent disclosure of confidential client information. This Committee agrees with Wisconsin's interpretation of Comments [18] and [19] to Rule 1.6, including its conclusion that:

> What information is protected and the exceptions that require or permit disclosure remain unchanged. What has changed, however, is the variety of circumstances under which the lawyer's responsibility to protect the information from unwarranted disclosure. Compliance with these duties can be complicated, particularly when the lawyer is working remotely, physically separated from co-workers, staff, and the information to be protected.

Id., p. 6.

E. Rules 5.1 and 5.3 (Responsibilities of Supervising Lawyers Regarding Lawyers and Nonlawyer Assistants)

Lawyers who have managerial or direct supervisory authority over other lawyers shall make reasonable efforts to ensure that the other lawyers conform to the Rules of Professional Conduct. *See* Colo. RPC 5.1(a) & (b). Rule 5.1 cmt. [2] 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." Rule 5.3 extends a lawyer's duty to supervise to the conduct of nonlawyers employed or associated with the lawyer. *See* Colo. RPC 5.3(a) & (b).

This Committee agrees with the ABA's conclusion that "[p]racticing virtually does not change or diminish [these] obligation[s]." ABA Opinion 498, p. 3. If anything, practicing virtually may enhance these obligations. Managerial lawyers practicing virtually

must create and tailor policies and practices that ensure all firm members and internal or external assistants operate in accordance with the lawyer's obligations that firm tasks are completed in a competent, timely, and secure manner. This can be accomplished by routine and frequent communication and other interactions with associates, legal assistants, and paralegals. Such connections "are also advisable to discern the health and wellness of the lawyer's team members." ABA Opinion 498, p. 7.

ABA Opinion 498 stresses the importance of supervising lawyers monitoring how lawyers and lawyer assistants use their own devices to access, transmit, or store client-related information. Security policies for personal device use should be heightened by: (1) requiring strong passwords for devices, routers, and to any virtual private network (VPN); (2) ensuring timely installation of updates; (3) ensuring the ability to remotely wipe any lost or stolen devices; (4) ensuring that staff member's family or others do not have access to client-related information; and (5) ensuring that client data and documents will be adequately and safely archived and available for later retrieval.

ABA Opinion 498 also cites the recommendations from the New York County Lawyers Association Ethics Committee for supervising lawyers to include in their firm's practices and policies. ABA Opinion 498, p. 6, n. 24. Representative examples include: (1) "[m]onitoring appropriate use of firm networks for work purposes;" (2) "[t]ightening off-site work procedures to ensure that the increase in worksites does not similarly increase the entry points for a data breach;" (3) "[m]onitoring adherence to firm cybersecurity procedures (e.g., not processing or transmitting work across insecure networks, and appropriate storage of client data and work product);" (4) "[e]nsuring that working at home

has not significantly increased the likelihood of an inadvertent disclosure;" and (5) having periodic check-ins. *Id.* (citing N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 754-2020, "Obligations When Lawyers Work Remotely" (2020)).

Wisconsin echoed the ABA's position, stating "[o]versight ... can be particularly challenging when those supervised are working in different, remote locations, separate from their supervisor and each other." Wisconsin Opinion 21-02, p. 7. To help achieve the level of supervision envisioned by the rules, the Wisconsin ethics committee suggests conducting regular videoconference meetings to develop structure to adhere to schedules, facilitate collaboration, and communication. Other strategies to facilitate remote work efficiencies include "[r]egular mandatory training, review of the circumstances of a remotely working lawyer, the assignment of experienced mentors to new lawyers, and the creation of teams." *Id.* Managing lawyers should consider which of these types of measures are appropriate in their work environment to ensure the people they supervise comply with the Rules and should communicate these policies clearly to employees.

F. Rule 5.5 (Unauthorized Practice of Law)

The pandemic greatly increased the number of lawyers practicing not only virtually, but remotely, away from the jurisdictions in which they were admitted. For example, a lawyer admitted to practice in Colorado might work remotely from a residence in Hawaii, even though the lawyer is not admitted to practice in Hawaii.

Rule 5.5 prohibits a lawyer from engaging in the unauthorized practice of law in other jurisdictions, among other things. Colo. RPC 5.5(a). Rule 5.5(a)(2) prohibits a lawyer from "practic[ing] law in a jurisdiction where doing so violates the regulation of

the legal profession in that jurisdiction…." Colo. RPC 5.5(a)(2).

A lawyer admitted to practice in Colorado who is considering practicing remotely in a jurisdiction where the lawyer is not admitted to practice therefore must determine whether the law of the other jurisdiction permits them to do so.[7] If a lawyer admitted to practice in Colorado practices remotely in a jurisdiction where the lawyer is not admitted to practice and the other jurisdiction does not permit remote practice, then the lawyer might be in violation of the law of both the other jurisdiction and Colo. RPC 5.5(a)(2).

ABA Formal Opinion 495 analyzes this issue through the framework of ABA Model Rule 5.5 and does not attempt to opine about the applicable law in all the states. *See* ABA Comm. On Ethics and Prof. Resp., Formal Op. 495, "Lawyers Working Remotely" (Dec. 16, 2020), p. 1. ABA Formal Opinion 495 concludes:

> It is not this Committee's purview to determine matters of law; thus, this Committee will *not* opine whether working remotely by practicing the law of one's licensing jurisdiction in a particular jurisdiction where one is not licensed constitutes the unauthorized practice of law under the law of that jurisdiction. If a particular jurisdiction has made the determination, by statute, rule, case law, or opinion, that a lawyer working remotely while physically located in that jurisdiction constitutes the unauthorized or unlicensed practice of law, then Model Rule 5.5(a) also would prohibit the lawyer from doing so.

Id. (emphasis added).

---

[7] The opinion is purposely limited to address this single scenario because Colorado lawyers are most likely to engage in this situation when practicing virtually. This opinion does not address other possible scenarios such as a lawyer licensed in and practicing the law of another jurisdiction while living in Colorado or a lawyer licensed in Colorado and living in Colorado while practicing the law of another jurisdiction in which they are licensed; *see also Can Out-of-State Attorneys Reside in Colorado?* Office of Attorney Regulation Newsletter (Colorado Supreme Court) November 2020.

Likewise, this Opinion does not opine about the law of other jurisdictions regarding remote practice and virtual practice. In general, though, jurisdictions that have addressed this issue have done so in different ways. At least ten states have addressed this issue through their state Rules, mostly their versions of Model Rule 5.5. These states are Arizona (Az. RPC 5.5(d)), Connecticut (Conn. RPC 5.5(f) & commentary), Hawaii (Hi. Rule 5.5, cmt. [3]), Minnesota (Mn. RPC 5.5(d)), New Hampshire (N.H. RPC 5.5(d)(3)), New York (N.Y. Ct. Rules, § 523.5 Working From Home), North Carolina (N.C. RPC 5.5(d)(2)), Ohio (Ohio RPC 5.5(d)(4) & cmt. [22]), South Carolina (S.C. RPC5.5, cmt. [4]), and Vermont (Vt. RPC 5.5 and Board's Note—2022 Amendment).

Other jurisdictions have addressed this issue by opinion. These are the District of Columbia (D.C. Comm. Unauthorized Practice L. Formal Op. 24-40 (2020)), Florida (Fla. Advisory Op.—Out of State Attorney Working Remotely from Florida Home, No. SC20-1220 (May 20, 2021)), Pennsylvania (Penn. & Phil. Bar Ass'ns, Joint Formal Op. 2021-100 (2021)), and New Jersey (N.J. Comm. on Unauthorized Practice of Law & N.J. Comm. on Prof'l Ethics, Joint Op. 59, "Non-New Jersey Licensed Lawyers Associated With Out-of-State Law Firms or Serving as In House Counsel to Out-of-State Companies Remotely Working from New Jersey Home" (Oct. 6, 2021).

IV. Considerations and Best Practices for Virtual Practice Technologies

Given the wide array of technical devices, services, and protections thereof, lawyers practicing virtually need to assess whether their technology, other assistance, and work environment are consistent with the Colorado Rules. With technology inevitably evolving, there is also an ongoing obligation to periodically assess whether existing systems are providing adequate adherence to the rules.

ABA Opinion 498 and opinions from other states provide guidance on specific virtual practice technologies a lawyer should consider when engaging in a virtual practice. To assist Colorado lawyers in making these assessments, adopting policies, and implementing appropriate training for attorney and non-attorney staff they supervise, this opinion summarizes suggested best practices for some common virtual practice tools.

A. Hardware/ Software

As a best practice for hardware, this Committee recommends that all devices (such as desktops computers, laptops, tablets, portable drives, phones, and scanners/copiers) be protected with security features and additional reasonable security measures. USB drives or other external hardware should be avoided unless they are owned or supplied by the firm or authorized by the firm and supplied by another trusted source. ABA Opinion 498, p. 11. Law firm managers should consider whether it is feasible for lawyers and staff to only use hardware issued by the firm or authorized by the firm.

Best practices include carefully reviewing licensing terms of service for both hardware and software systems to ensure client confidentiality is protected. "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." *Id.*, p. 4, n. 17. [8]

The duty to evaluate a vendor's terms and services to determine whether they adequately protect client information includes consulting with someone qualified to make such an assessment if the lawyer cannot do so independently. Virginia Opinion 1872, p. 1. [9] ABA Opinion 498 states that lawyers may also need to rely on information from technology professionals and vendors for general assistance and lawyers must ensure that these individuals and companies comply with confidentiality and other ethical duties. In such circumstances, the ABA suggests that "[w]hen appropriate, lawyers should consider use of a confidentiality agreement, and should ensure that all client-related information is secure, indexed, and readily retrievable." ABA Opinion 498, p. 7.[10] The Virginia and ABA opinions are based upon ABA Model Rule 1.6(b)(6),[11] which does not have a similar

---

[8] *See also INSIGHT: Zooming and Attorney Client Privilege* (lawyers must understand that if video conferences are recorded, the vendor may retain a copy under the terms of service), article available at https://www.google.com/search?q=INSIGHT%3A+Zooming+and+Attorney+Client+Privilege&rlz=1C1GCEJ_enUS1028US1028&oq=INSIGHT%3A+Zooming+and+Attorney+Client+Privilege&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQRRg60gEHNTg2ajBqNKgCALACAA&sourceid=chrome&ie=UTF-8.

[9] *See also* VA Legal Ethics Opinion 1818, "Whether the Client's File May Contain Only Electronic Documents With No Paper Retention?" (Sept. 30, 2005) (concluding "that a lawyer could permissibly store files electronically and destroy all paper documents as long as the client was not prejudiced by this practice, but noted that the lawyer may need to consult outside technical assistance and support for assistance in using such a system.").

[10] *See also* Mo. Bar Informal Advisory Op. 20070008 (opining that "[i]t is permissible" for a lawyer to contract with a third party vendor to electronically scan closed files to store them); Mo. Bar Informal Advisory Op. 20050068 (opining it is permissible for lawyer "to hire an answering service to answer phones during non-business hours" as long as lawyer makes reasonable provisions and enters into appropriate agreements to protect client confidentiality).

[11] VA RPC 1.6(b)(6) states "[t]o the extent a lawyer reasonably believes necessary, the lawyer

counterpart in the Colorado Rules. Utilizing outside professionals to evaluate technology methods, systems, and security, therefore, is not a requirement in Colorado but rather a prudent practice a lawyer may want to consider.

B. Accessing Client Files and Data

Lawyers working remotely must have reliable and consistent access to client records and files. If such information is accessed 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." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 "Ethical Obligations Related to Disasters" (Sept. 19, 2018). In addition to requiring a strong password, a reasonable precaution to reduce the likelihood of unauthorized access to firm information and firm networks is to use multi-factor authentication. Wisconsin Opinion 21-02, p. 10. Lawyers should also make sure that client data is regularly backed up and that secure access to backup data is available in the event of a data loss. Finally, lawyers should be aware of any statutory requirements regarding data breaches and consider adopting a corresponding data breach policy in case data is lost or hacked and a plan for disclosing data losses or breaches to impacted clients.[12]

---

may reveal … information to an outside agency necessary for … office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential."

[12] *See* ABA Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack* (2018); *see also* C.R.S. § 6-1-716 (requiring notification of security breach); C.R.S. § 6-1-713(1) (requiring "[e]ach covered entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic

C. Virtual Meeting and Videoconferencing Platforms

For video conferencing services, lawyers should explore whether a virtual meeting platform offers higher tiers of security for businesses/enterprises plans compared to its free or consumer platform plans. Any recordings or transcripts should be secured and, if the platform will be recording conversations with the client, then client consent is required.[13] To avoid jeopardizing the attorney-client privilege and violating the duty of confidentiality, the lawyer should take steps so that client-related meetings are not overheard or seen by third parties in the household or other remote locations unless the third parties are assisting with the representation.

Multiple opinions cite the following steps recommended by the FBI to provide adequate security for video meetings and conferences: "use the up-to-date version of the application; do not make the meetings public; require a meeting password; do not share the link to the video meeting on an unrestricted publicly available social media post; provide the meeting link directly to the invited guests; and manage the screen-sharing options." Wisconsin Opinion 21-02, p. 12.[14]

D. Virtual Document and Data Exchange Platforms

Platforms that exchange virtual document and data need to appropriately archive the

---

documents containing personal identifying information."); C.R.S. § 6-1-713.5 (providing for protection of personal identifying information). The applicability and application of these statutes is beyond the scope of this opinion.

[13] *See* CBA Formal Op. 112, "Surreptitious recording of conversations or statements" (July 2003).

[14] *See also* Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2020-300, "Ethical Obligations for Lawyers Working Remotely" (2020). The FBI article can be found here: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-oftelecon ferencing-andonline-classroom-hijacking-during-covid-19-pandemic.

documents and data for later retrieval and ensure that the service remains secure. Additionally, a lawyer should consider whether the information being transmitted is or needs to be encrypted, both in transit and in storage.

ABA Opinion 477R provides guidance on these issues. In the opinion, the ABA reasoned that the use of unencrypted routine email is generally an acceptable method of exchanging lawyer-client communication because "unencrypted email poses no greater risk of interception or disclosure than other non-electronic forms of communication." ABA Opinion 477R, p. 5. The opinion also cautions, however, that it is not always reasonable to rely on the use of unencrypted email due to cyber-threats and the proliferation of other electronic communications devices, such as mobile applications, message boards, and unsecured networks, which may lack the basic expectation of privacy afforded to email communications. *Id.* Lawyers must therefore continuously consider on a case-by-case basis how they virtually exchange documents and data about client matters by applying the reasonableness factors contained in Rule 1.6 cmt. [18], discussed in Section III(D) above.

In addition to documents and data exchanged by email, lawyers should not open suspicious attachments or click unusual links in text messages, posts, online ads, or other forms of communication. A lawyer should also consider using websites that have enhanced security, such as those beginning with "HTTPS" rather than "HTTP,"[15] where practical.

E. Smart Speakers, Virtual Assistants, and Listening- Enabled Features

Lawyers should be aware that devices and services such as smart speakers and

[15] Wisconsin Opinion 21-02, p. 11.

virtual assistants have listening capabilities, as well as the ability to record conversations.[16] These devices and features therefore should be disabled unless the technology is used to assist the lawyer's practice and the lawyer has ensured that the applicable terms of service adequately protect client confidentiality. Failure to do so exposes client and other sensitive information to unnecessary and unauthorized third parties and increases the risk of hacking.

V. Conclusion

The post pandemic world is a different environment for many lawyers by allowing them greater opportunities to practice virtually, either in full or in part. These opportunities, however, are accompanied by unique ethical considerations under the Colorado Rules of Professional Conduct, which apply uniformly to lawyers who work in physical offices and those who practice virtually. In particular, virtual practice may create new challenges when ensuring a lawyer's compliance with their obligations of competence, diligence, proper communication, confidentiality, supervision of other lawyers and nonlawyers, and the unauthorized practice of law.

[16] *See* ABA Opinion 498, p. 6; *see also* Wisconsin Opinion 21-02, p. 12 (discussing these features and the risks and benefits associated with them).