



AMERICAN
BANKRUPTCY
INSTITUTE

Northeast Bankruptcy Conference and Consumer Forum

Consumer Track

Ethics Potpourri

Christine E. Devine

Law Office of Christine E. Devine LLC | Medway, Mass.

William K. Harrington

Office of the U.S. Trustee | New York

Hon. Enrique S. Lamoutte

U.S. Bankruptcy Court (D. P.R.) | San Juan

Adam J. Ruttenberg

Beacon Law Group, LLC | Needham, Mass.

Ethics Potpourri

2023 ABI Northeast Bankruptcy Conference & Consumer Forum

PANELISTS

Judge Enrique S. Lamoutte Inclán
William K. Harrington, U.S. Trustee
Christine E. Devine, Esq.
Adam J. Ruttenberg, Esq.

Overview

Certain Relevant ABA Model Rules

- Model Rule 1.1 – Competence
- Model Rule 1.4 – Communication
- Model Rule 1.6 – Confidentiality
- Model Rule 5.1, 5.2, and 5.3 – Supervision
- Model Rule 5.5 – Unauthorized Practice of Law

Overview

Certain Relevant ABA Ethics Opinions

- Formal Opinion 477R – Securing Communication of Protected Client Information
- Formal Opinion 483 – Lawyers’ Obligations After an Electronic Data Breach of Cyberattack
- Formal Opinion 495 – Lawyers Working Remotely
- Formal Opinion 498 - Virtual Practice

I. Initial Client Meeting

Scenario:

After a few phone calls about the possibility of a personal Chapter 7 filing, Counsel has an initial “meeting” with the new client (and spouse) by Zoom and, with the flexibility of video meetings, Counsel conducts the meeting from an out of state vacation home.

A Few Issues To Consider:

- Special Challenges When Practicing Law From Home
- Verifying Client Identity
- Exchanging Documents

Rules Implicated / Considerations

- Practicing Law From An Out of State Vacation Home
 - Consider Model Rule 5.5 – Unauthorized Practice of Law
 - Addressed In ABA Formal Opinions 495 and 498
- Verifying Client Identity
 - Requirements of the U.S. Trustee
 - Electronic Filing Requirements – Efiling Declarations
- Exchanging Documents
 - Consider Model Rule 1.1 – Competence, Including Comment 8
 - Consider Model Rule 1.6 – Confidentiality
 - Addressed In ABA Formal Opinion 477R

II. Final Review and Meeting to Sign

Scenarios:

After the initial Zoom meeting with both clients, Counsel prepares the bankruptcy petition and schedules and has a final meeting to verify details, but one spouse never actually appears on screen.

After the meeting, multiple signatures pages only arrive, signed by the clients, multiple copies of each, with a sticky note to “apply wherever required”.

After the meeting, Counsel realizes some final edits are required and asks a paralegal to make the changes. The paralegal agrees finishes the edits at home from using the family computer.

Rules Implicated / Considerations

- Verifying Client Identity
 - Requirements of the U.S. Trustee
- Client Consent / Authorization Issues
 - Consider Model Rule 1.4 – Communications
- Paralegal Working From Home
 - Consider Model Rule 1.6 - Confidentiality
 - Consider Model Rule 5.1 and 5.3 – Supervisory Issues

III. Section 341 Meeting

Scenarios:

The Trustee conducts the Section 341 Meeting by telephone and clients are present in the office with Counsel. As the Trustee digs in on a particular issue regarding an asset, the client makes repeated gestures and passes notes to counsel.

Rules Implicated / Considerations

- Notes and Gestures During the Meeting
 - Consider Model Rule 3.3 – Candor toward the Tribunal
 - Consider fairness to creditors / Trustee

IV. Counsel is Hacked

Scenario:

Counsel realizes that the computer network, which contains confidential client information, has been hacked.

Rules Implicated / Considerations

- Data breach Generally
 - Consider Model Rule 5.1 and 5.3 , Including Relevant Comments – Duty of Supervision
 - Consider Model Rule 1.1 – Competence, Including Comment 8
 - Consider Model Rule 1.6 – Confidentiality
 - Addressed In ABA Formal Opinion 483
- Obligation to Provide Notice After a Breach
 - Consider Model Rule 1.4 - Communications
 - Consider Model Rule 1.9 – Duties to Former Clients
 - Addressed In ABA Formal Opinion 483
 - See also ABA Formal Opinion 477R

V. Use of Artificial Intelligence

Scenario:

During Counsel's argument before the Court, the Judge asks for confirmation of certain citation in Counsel's brief. Counsel had worked with a team of colleagues on the research and told the Judge they would provide copies of all cases cited within a week. Unfortunately, counsel learned that a colleague had provided the facts of the matter to ChatGPT and then used the citations provided in the brief.

Rules Implicated / Considerations

Use of AI, Chat GPT

- Consider Model Rule 1.1 – Competence
- Consider Model Rule 1.6 – Confidentiality
- Consider Model Rule 5.1 and 5.3 – Supervisory Issues (when relying on information provided by others)
- Consider: Benjamin Weiser, *Here's What Happens When Your Lawyer Uses ChatGPT*, The New York Times (May 27, 2023)



Enjoy Newport!



Northeast Bankruptcy Conference & Consumer Forum July 13 – 15, 2023 / Newport R.I.

ETHICS POTPOURRI

**Enrique S. Lamoutte Inclán
U. S. Bankruptcy Judge
District of Puerto Rico**

INTRODUCTION

The advancement of technology and the preservation of ethical values present a challenge to all professionals, including legal practitioners, as they appear to be dancing at a different pace and rhythm. It is not difficult to determine which is moving at a faster pace, technology.

The coronavirus pandemic has heightened the need to understand the ethical implications our current scenario presents. Technology has allowed the legal practice to attend to the need of our society to access the judicial system through improvements in remote practice, digital filings, and virtual hearings.

However, lawyers must be aware of how the technological advancements that are needed to meet the pandemic crisis affect their ethical rules of conduct, particularly, those of the state wherein they practice, in conjunction with the Model Rules of Professional Conduct of the American Bar Association (“Model Rules”).

The main objective of this Panel is to create such awareness and to promote responsiveness to the ethical challenges of any crisis, and, particularly, the coronavirus pandemic crisis and the use of Artificial Intelligence (“AI”) powered chatbots in the legal profession.

ETHICS

Ethics, management, and good advocacy are interrelated subjects with one common purpose, that is, doing things well. Experience has proven that ethics and competence go hand in hand. Model Rule 1.1 (Competence) states that “[a] lawyer shall provide competent

representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.”

A lawyer is in a unique position. The lawyer represents a client, is an officer of the court, and, many times, is also a public servant. In the interaction and balance of the three duties lie most ethical problems, because ethics is a matter of choices. See Preamble to the Model Rules.

An attorney is not under any obligation to assume the representation of a client. However, when the representation is accepted, either explicitly or impliedly, an attorney must comply with the Model Rules or whatever ethical rules are in effect in the court where the attorney appears. The Model Rules generally contain an element of cognition. The lawyer must be aware of the client-lawyer relationship.

Ethical problems often arise when an attorney’s duty to a client outweighs the duty of candor to the Court and overshadows the traditional notions of advocacy and professionalism. Ethical responsibilities may limit zealous advocacy. Ethics have a distinct and major impact in bankruptcy law. The bankruptcy subject matter inevitably touches business decisions, affects many parties, and, generally, time is of the essence. Special awareness of the Model Rules is necessary in asset protection planning. The above statements are logical and generally accepted. The problem lies in applying them to a particular set of facts.

ETHICS AND THE COVID-19 PANDEMIC

The coronavirus pandemic has affected us all in many ways. The legal profession must adjust to the changed environment, develop new approaches, and implement protocols that meet the obligations and responsibilities of competence, confidentiality, diligence, supervision, and unauthorized practice of law.

Technology and the use of artificial intelligence will continue to advance. Artificial intelligence tools are already present in the legal profession. The extent of their impact depends on our willingness as legal professionals to learn how to use the technology tools. ChatGPT, a chatbot model that combines artificial intelligence and natural language with an enormous dataset of text, is here. ChatGPT is a chatbot that uses artificial intelligence (AI) and natural language to create humanlike dialogue. GPT stands for Generative Pretrained Transformer which is a type of large language model. A chatbot is a computer program designed to simulate conversation with human users, especially over the internet. ChatGPT, and other programs like it, open new ways to access information that have and will inevitably change the practice of law at all levels. Model Rule 1.1 imposes a duty of competence. It behooves attorneys to learn how to use artificial intelligence tools in an ethical manner. The ethics of professional conduct in the legal profession must develop in a manner consistent with artificial intelligence ethics.

On May 30, 2023, CNN published an article, titled “AI industry and researchers sign statement warning of ‘extinction risk.’” The article is a response by leading industry officials including Open AI CEO Sam Altman (the “godfather” of AI); Geoffrey Hinton; top executives from Google DeepMind and Anthropic; Kevin Scott, Microsoft’s chief technology

officer; Bruce Schneier, the internet security and cryptography pioneer, amongst others to warn about concerns regarding the ultimate danger of unchecked artificial intelligence. Given the viral success of Open AI's ChatGPT, these industry experts are calling for regulation. Moreover, "... a growing number of lawmakers, advocacy groups and tech insiders have raised alarms about the potential for a new crop of AI powered chatbots to spread misinformation and displace jobs." "Dan Hendrycks, director of the Center for AI Safety, said in a tweet Tuesday that the statement first proposed by David Krueger, an AI professor at the University of Cambridge, does not preclude society from addressing other types of AI risks, such as algorithmic bias or misinformation."

Recent articles have raised a red flag on attorneys using ChatGPT. One example is of a New York licensed attorney who used ChatGPT to supplement a brief, and the same cited to numerous cases that the AI model made up, did not exist, and could not be located by opposing counsel nor the presiding judge. See: Debra Cassens Weiss, Judge finds out why brief cited nonexistent cases – ChatGPT id research, ABA Journal, Weekly Newsletter, June 2, 2023; Benjamin Weiser, Here's What Happens When Your Lawyer Uses ChatGPT, The New York Times (May 27, 2023); and Matt Novak, Lawyer Uses ChatGPT In Federal Court And It Goes Horribly Wrong, Forbes (May 27, 2023).

Technology, automation, and artificial intelligence are tools to improve data collection, but not a substitute to human judgment. It is the ultimate responsibility of the legal professional to apply data effectively and efficiently. The responsibility is discharged using individual judgment. Algorithmic decision-making may appear to be an objective result to a problem. However, the use of human judgment is indispensable to preserve ethical concerns and the changing philosophical views of our society.

The interaction of humans and machines has been a part of our lives and will continue to be. The current developments give rise to new ethical dilemmas. We must be aware of them and establish mechanisms to build solutions that serve our citizens and promote a better future. Technological advancements have also made cybersecurity a challenge for attorneys and legal firms to protect against a threat environment on private data. Attorneys and law firms must be aware of such threats and implement cybersecurity programs, policies, and procedures. Attorneys have the ethical duty to take competent and reasonable measures to safeguard information of clients, particularly, confidential information. See Model Rules 1.1 (Competence), 1.4 (Communication), 1.6 (Confidentiality); and Model Rules 5.1, 5.2 and 5.3 (Supervision).

Crisis is not an unknown factor to attorneys as a client's crisis is what prompts the client to seek legal advice. However, an unprecedented general crisis may affect an attorney's ability to respond to a client's crisis. The spread of technology and the coronavirus pandemic are factors that present a "crisis" which needs special attention from an attorney. The Model Rules provide an excellent guidance to attorneys. See Raymond H. Brescia, Ethics In Pandemics: The Lawyer for the (Crisis) Situation, The Georgetown Journal of Legal Ethics, Vol. 34:295 (2021).

The rules of professional conduct apply in time of crisis, such as the Covid-19 pandemic. Confidentiality in an office setting was the normal procedure to comply with Model Rule 1.6. While technology has developed in all professional fields, including law-related services, the

need to hold meetings via Teams or Zoom platform presents a challenge to protect confidentiality. The use of technology to meet the pandemic crisis carries operational costs. Thus, attorneys must comply with Model Rule 1.5

Attorneys must also ensure that their law-related services do not violate Model Rule 5.7, which prohibits the unauthorized practice of law.

There are ABA Ethics Opinions that set the basis and illustrate how to meet the ethical challenges of technology and the coronavirus pandemic. I will refer to the following four Formal Opinions: 477R (May 11, 2017); 483 (October 17, 2018); 495 (December 16, 2020); and 498 (March 10, 2021).

- **Formal Opinion 477R**

ABA Formal Opinion 477R describes the current threat environment: “Cybersecurity recognizes a ... world where law enforcement discusses hacking and data loss in terms of ‘when,’ and not ‘if’...” a company (or law firm) will be breached.

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and often have contractual and regulatory duties to protect confidential information.

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

- **Formal Opinion 483**

ABA Formal Opinion 483, titled “Lawyers’ Obligations After an Electronic Data Breach or Cyberattack”, reviews lawyers’ duties of competence, communication, confidentiality, and supervision in safeguarding confidential data and in responding to data breaches. It finds that Model Rule 1.15 (Safeguarding Property) applies to electronic client files as well as paper client files and requires the care required of a professional fiduciary.

The Opinion states that these duties include: The obligation to monitor for a breach, the duty to stop a breach and restore systems, and the duty to determine what happened.

The Opinion uses the following definition of a data breach: “a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.” It is important to note that the terms “security event,” “security incident,” and “data breach” sometimes have different meanings in various security standards and frameworks, laws and

regulations, and contracts. It is, accordingly, important to understand the context and any applicable definitions when viewing and using these terms.

Although it does not impose a requirement for an incident response plan, the Opinion suggests “as a matter of preparation and best practices” that “lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.”

The Opinion finds that attorneys have a duty under Model Rule 1.4 to communicate with current clients concerning a data breach. Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach. Applying Model Rule 1.9(c), the Opinion finds no requirement to notify a former client of a breach “as a matter of legal ethics.”

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.

Comment: I would strongly recommend having Cybersecurity insurance, as Model Rule 1.6(c) requires “reasonable efforts to prevent unauthorized disclosure.” There are two types of cybersecurity insurance: (i) first-party cyber liability insurance – provides coverage for the direct financial impact of a breach or cyber-attack in the network or system (may include lost income during downtime, the fees for restoring data, forensic investigations, etc.); and (ii) third-party liability insurance protects law firms from liability claims in the event of a breach (may include payments to clients or regulatory fines for noncompliance).

- **Formal Opinion 495**

ABA Formal Opinion 495, holds that a lawyer can practice law while physically outside the jurisdiction in which she is licensed to practice, provided she follow “specific parameters.”

Lawyers 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. This practice may include the law of their licensing jurisdiction or other law as permitted by Model Rule 5.5(c) or (d) including, for instance, temporary practice involving other states or federal laws. Having local contact information on websites, letterhead, business cards, advertising, or the like would improperly establish a local office or local presence under the Model Rules.

Thus, a lawyer admitted in one jurisdiction, but working remotely in another jurisdiction in which he or she is not admitted, should follow the conclusions of ABA Formal Opinion 495, and should determine whether the jurisdiction in which the lawyer is working remotely constitutes the unauthorized practice of law under the law of that jurisdiction.

- **Formal Opinion 498**

ABA Formal Opinion 498 applies the now well-established principles that lawyers must reasonably stay abreast of the benefits and risks of technology, make reasonable efforts to avoid breaches of confidentiality, and implement policies to ensure that subordinate lawyers and staff do the same.

This Opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional law firm. A lawyer's virtual practice often occurs when a lawyer 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 have a physical office separate from their dwelling or residence.

Concerning competence, diligence, and communication "a lawyer should keep abreast of changes in the law and practice, including the benefits and risks associated with relevant technology . . ."

Confidentiality requires "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." The Opinion lists several factors to be considered by the lawyer, but generally concludes that the lawyer may communicate about the client's representation over the Internet if reasonable efforts were made to prevent unauthorized or inadvertent access.

Supervision, exercise of managerial authority, in a virtual practice still requires reasonable efforts to "ensure that subordinate lawyers and non-lawyer assistants comply with the applicable Rules of Professional Conduct." Lawyers are required to provide appropriate instruction and supervision concerning the ethical obligations of their employment, including the obligation to safeguard the client's confidences.

The Opinion provides guidance concerning practice technologies and considerations. Issues concern hard/software systems, accessing client files and data, virtual meeting platforms and video conferencing, virtual document and data exchange platforms,

and smart speakers, virtual assistants and other listening enabled devices are presented, and guidance provided. The Opinion also lists possible limitations of virtual practice.

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.

IN-PRESENCE HEARINGS

I recommend that the courts implement in-presence hearings to a degree consonant with the current state of the pandemic in their district. The past three years have presented a challenge to all institutions, including the bankruptcy courts. The challenge has caused the bankruptcy courts to change operational procedures and to make a better use of technology. Bankruptcy courts have done well. Clearly, court operations are facing a new post-pandemic world. It is unlikely that we will ever go back to how operations were conducted before March 2020. I foresee that bankruptcy courts will continue to use enhanced technology, such as hearings and meetings via Teams, Zoom, or any other platform. However, in presence hearings and personal interaction between and among the staff, at all levels, and attorneys appearing at in presence at hearings are necessary to maintain our structural and institutional strength. The judiciary system has a duty to project standards of independence and integrity, as they are indispensable to its image before the society they serve.

There is value to in presence meetings and hearings. Interpersonal interaction captures attention and promotes participants to engage in collaboration, increases morale and improves work satisfaction. Technological advances have also improved the access to the judicial system. Courts must balance the two to reach the ultimate objective of access to and imparting justice. Courts must identify the proceedings that lend themselves to virtual/remote hearings and those that should be held in presence.

The capabilities of technology have developed and improved, but dependency on it has also increased. Innovations in technology have been critical to the progress and accomplishments of our courts. Technology has allowed us to connect during the pandemic with one another through the Internet using the Microsoft Teams and Zoom platforms. It has improved the ability to work remotely, travel while working, and constantly stay in touch with our peers while physically being in a different state or country. However, technology has also prompted gaps between one another in our interpersonal relationships and the image of the judicial system.

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.

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 498

2

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].

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 498

4

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).

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 498**6**

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

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 498**8**

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.”).

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 495

December 16, 2020

Lawyers Working Remotely

Lawyers 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. This practice may include the law of their licensing jurisdiction or other law as permitted by ABA Model Rule 5.5(c) or (d), including, for instance, temporary practice involving other states' or federal laws. Having local contact information on websites, letterhead, business cards, advertising, or the like would improperly establish a local office or local presence under the ABA Model Rules.¹

Introduction

Lawyers, like others, have more frequently been working remotely: practicing law mainly through electronic means. Technology has made it possible for a lawyer to practice virtually in a jurisdiction where the lawyer is licensed, providing legal services to residents of that jurisdiction, even though the lawyer may be physically located in a different jurisdiction where the lawyer is not licensed. A lawyer's residence may not be the same jurisdiction where a lawyer is licensed. Thus, some lawyers have either chosen or been forced to remotely carry on their practice of the law of the jurisdiction or jurisdictions in which they are licensed while being physically present in a jurisdiction in which they are not licensed to practice. Lawyers may ethically engage in practicing law as authorized by their licensing jurisdiction(s) while being physically present in a jurisdiction in which they are not admitted under specific circumstances enumerated in this opinion.

Analysis

ABA Model Rule 5.5(a) prohibits lawyers from engaging in the unauthorized practice of law: "[a] lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or assist another in doing so" unless authorized by the rules or law to do so. 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

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.

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 495

2

the unauthorized or unlicensed practice of law, then Model Rule 5.5(a) also would prohibit the lawyer from doing so.

Absent such a determination, this Committee's opinion is that a lawyer may practice law pursuant to the jurisdiction(s) in which the lawyer is licensed (the "licensing jurisdiction") even from a physical location where the lawyer is not licensed (the "local jurisdiction") under specific parameters. Authorization in the licensing jurisdiction can be by licensure of the highest court of a state or a federal court. For purposes of this opinion, practice of the licensing jurisdiction law may include the law of the licensing jurisdiction and other law as permitted by ABA Model Rule 5.5(c) or (d), including, for instance, temporary practice involving other states' or federal laws. In other words, the lawyer may practice from home (or other remote location) whatever law(s) the lawyer is authorized to practice by the lawyer's licensing jurisdiction, as they would from their office in the licensing jurisdiction. As recognized by Rule 5.5(d)(2), a federal agency may also authorize lawyers to appear before it in any U.S. jurisdiction. The rules are considered rules of reason and their purpose must be examined to determine their meaning. Comment [2] indicates the purpose of the rule: "limiting the practice of law to members of the bar protects the public against rendition of legal services by unqualified persons." A local jurisdiction has no real interest in prohibiting a lawyer from practicing the law of a jurisdiction in which that lawyer is licensed and therefore qualified to represent clients in that jurisdiction. A local jurisdiction, however, does have an interest in ensuring lawyers practicing in its jurisdiction are competent to do so.

Model Rule 5.5(b)(1) prohibits a lawyer from "establish[ing] an office or other systematic and continuous presence in [the] jurisdiction [in which the lawyer is not licensed] for the practice of law." Words in the rules, unless otherwise defined, are given their ordinary meaning. "Establish" means "to found, institute, build, or bring into being on a firm or stable basis."² A local office is not "established" within the meaning of the rule by the lawyer working in the local jurisdiction if the lawyer does not hold out to the public an address in the local jurisdiction as an office and a local jurisdiction address does not appear on letterhead, business cards, websites, or other indicia of a lawyer's presence.³ Likewise it does not "establish" a systematic and continuous presence in the jurisdiction for the practice of law since the lawyer is neither practicing the law of the local jurisdiction nor holding out the availability to do so. The lawyer's physical presence in the local jurisdiction is incidental; it is not for the practice of law. Conversely, a lawyer who includes a local jurisdiction address on websites, letterhead, business cards, or advertising may be said to have established an office or a systematic and continuous presence in the local jurisdiction for the practice of law.

Subparagraph (b)(2) prohibits a lawyer from "hold[ing] out to the public or otherwise represent[ing] that the lawyer is admitted to practice law in [the] jurisdiction" in which the lawyer is not admitted to practice. A lawyer practicing remotely from a local jurisdiction may not state or imply that the lawyer is licensed to practice law in the local jurisdiction. Again, information provided on websites, letterhead, business cards, or advertising would be indicia of whether a lawyer is "holding out" as practicing law in the local jurisdiction. If the lawyer's website,

² DICTIONARY.COM, <https://www.dictionary.com/browse/establish?s=t> (last visited Dec. 14, 2020).

³ To avoid confusion of clients and others who might presume the lawyer is regularly present at a physical address in the licensing jurisdiction, the lawyer might include a notation in each publication of the address such as "by appointment only" or "for mail delivery."

letterhead, business cards, advertising, and the like clearly indicate the lawyer's jurisdictional limitations, do not provide an address in the local jurisdiction, and do not offer to provide legal services in the local jurisdiction, the lawyer has not "held out" as prohibited by the rule.

A handful of state opinions that have addressed the issue agree. Maine Ethics Opinion 189 (2005) finds:

Where the lawyer's practice is located in another state and where the lawyer is working on office matters from afar, we would conclude that the lawyer is not engaged in the unauthorized practice of law. We would reach the same conclusion with respect to a lawyer who lived in Maine and worked out of his or her home for the benefit of a law firm and clients located in some other jurisdiction. In neither case has the lawyer established a professional office in Maine, established some other systematic and continuous presence in Maine, held himself or herself out to the public as admitted in Maine, or even provided legal services in Maine where the lawyer is working for the benefit of a non-Maine client on a matter focused in a jurisdiction other than Maine.

Similarly, Utah Ethics Opinion 19-03 (2019) states: "what interest does the Utah State Bar have in regulating an out-of-state lawyer's practice for out-of-state clients simply because he has a private home in Utah? And the answer is the same—none."

In addition to the above, Model Rule 5.5(c)(4) provides that lawyers admitted to practice in another United States jurisdiction and not disbarred or suspended from practice in any jurisdiction may provide legal services on a temporary basis in the local jurisdiction that arise out of or reasonably relate to the lawyer's practice in a jurisdiction where the lawyer is admitted to practice. Comment [6] notes that there is no single definition for what is temporary and that it may include services that are provided on a recurring basis or for an extended period of time. For example, in a pandemic that results in safety measures—regardless of whether the safety measures are governmentally mandated—that include physical closure or limited use of law offices, lawyers may temporarily be working remotely. How long that temporary period lasts could vary significantly based on the need to address the pandemic. And Model Rule 5.5(d)(2) permits a lawyer admitted in another jurisdiction to provide legal services in the local jurisdiction that they are authorized to provide by federal or other law or rule to provide. A lawyer may be subject to discipline in the local jurisdiction, as well as the licensing jurisdiction, by providing services in the local jurisdiction under Model Rule 8.5(a).

Conclusion

The purpose of Model Rule 5.5 is to protect the public from unlicensed and unqualified practitioners of law. That purpose is not served by prohibiting a lawyer from practicing the law of a jurisdiction in which the lawyer is licensed, for clients with matters in that jurisdiction, if the lawyer is for all intents and purposes invisible *as a lawyer* to a local jurisdiction where the lawyer is physically located, but not licensed. The Committee's opinion is that, in the absence of a local jurisdiction's finding that the activity constitutes the unauthorized practice of law, a lawyer may practice the law authorized by the lawyer's licensing jurisdiction for clients of that jurisdiction,

CENTRAL STATES BANKRUPTCY WORKSHOP 2021

Formal Opinion 495

4

while physically located in a jurisdiction where the lawyer is not licensed if the lawyer does not hold out the lawyer's presence or availability to perform legal services in the local jurisdiction or actually provide legal services for matters subject to the local jurisdiction, unless otherwise authorized.

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

©2020 by the American Bar Association. All rights reserved.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R*

May 11, 2017

Revised May 22, 2017

Securing Communication of Protected Client Information

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. However, 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.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for email communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."¹

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.²

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 477R**2**

computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.³

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."⁴ Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.⁵

The 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.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."⁶ The scope of this requirement was

3. See JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

4. "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/cybersecurity> (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁷

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.⁸

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise.⁹ The 2012 modification added a new duty in paragraph (c) that: “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.”¹⁰

7. *Id.* at 43.

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.”

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 477R

4

Amended Comment [18] explains:

Paragraph (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. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.¹¹

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.¹²

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

the sensitivity of the information,

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

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).¹³

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.¹⁴ Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

14. See item 3 below.

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 477R**6**

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.¹⁵ "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As Comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. 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

15. See, e.g., Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/>.

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. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,¹⁶ and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client’s lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

16. See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 477R

8

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.¹⁷ If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.¹⁸

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.¹⁹

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

17. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One’s Client (2011). Formal Op. 11-459 was issued prior to the 2012 amendments to Rule 1.6. These amendments added new Rule 1.6(c), which provides that lawyers “shall” make reasonable efforts to prevent the unauthorized or inadvertent access to client information. *See, e.g.*, Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer’s email server).

18. Some state bar ethics opinions have explored the circumstances under which email communications should be afforded special security protections. *See, e.g.*, Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer...;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

19. *See* Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

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.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 477R

10

the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.²⁰

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

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.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”²¹ If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.²²

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

20. MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at:
http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2016). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012),
http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.auth_checkdam.pdf.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.²³ The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [19] to Model Rule 1.6, “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

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. However, 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.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

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

CHAIR: Myles V. Lynk, Tempe, AZ ■ John M. Barkett, Miami, FL ■ Arthur D. Burger, Washington, DC ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Robert A. Creamer, Cambridge, MA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Hope Cahill Todd, Washington, DC ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel; Mary McDermott, Associate Ethics Counsel

©2017 by the American Bar Association. All rights reserved.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).

AMERICAN BANKRUPTCY INSTITUTE

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

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.

Introduction¹

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.² In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.³ Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.⁴

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.⁵ This

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

² See, e.g., Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), <https://www.cio.com> (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); See also *Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

³ Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), <https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504>.

⁴ Robert S. Mueller, III, *Combating Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>.

⁵ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,⁶ and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.⁷

⁶ The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. See MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

⁷ In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") See also, e.g., *Cybersecurity Resources*, ABA Task Force on Cybersecurity, <https://www.americanbar.org/groups/cybersecurity/resources.html> (last visited Oct. 5, 2018).

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483

3

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁸ The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁹

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.¹⁰

⁸ MODEL RULES OF PROF’L CONDUCT R. 1.1 (2018).

⁹ A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

¹⁰ ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_a_mended_authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.¹¹

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

¹¹ MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483

5

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such 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.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data¹² and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,¹³ whether further action is warranted,¹⁴ whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,¹⁵ and how and when the lawyer must take further action under other regulatory and legal provisions.¹⁶ Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.¹⁷

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

¹² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008).

¹³ Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), available at <https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx> (noting that “[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization’s IT environment.”).

¹⁴ MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).

¹⁵ See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).

¹⁶ The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, <https://www.us-cert.gov/ais> (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

¹⁷ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.¹⁸ The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”¹⁹ While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm’s network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

¹⁸ See ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

¹⁹ NIST Computer Security Incident Handling Guide, at 6 (2012), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483

7

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.²⁰

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."²¹ These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

²⁰ Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

²¹ We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).²² Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.²³ The 2012 modification added a duty in paragraph (c) that: "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."²⁴

Amended Comment [18] explains:

Paragraph (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. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- 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

²² The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

²³ MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

²⁴ *Id.* at (c).

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483

9

- 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).²⁵

As this Committee recognized in ABA Formal Opinion 477R:

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney’s competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.²⁶ Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.²⁷ As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.²⁸

²⁵ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

²⁶ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

²⁷ MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”)

²⁸ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.²⁹ In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.³⁰ We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.³¹

²⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

³⁰ This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

³¹ Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483**11**

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”³² The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).³³

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.³⁴

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.”) (*citations omitted*).

³² ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

³³ *Id.*

³⁴ MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer” Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.”

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

AMERICAN BANKRUPTCY INSTITUTE

2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”³⁵ When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.³⁶

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.³⁷ We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.³⁸ Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

³⁵ MODEL RULES OF PROF’L CONDUCT R. 1.9(c)(2) (2018).

³⁶ See *Discipline of Feland*, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).

³⁷ See MODEL RULES OF PROF’L CONDUCT R. 1.9, cmt. [9] (2018).

³⁸ See ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.³⁹

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

³⁹ Cf. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

AMERICAN BANKRUPTCY INSTITUTE

Formal Opinion 483

15

information.⁴⁰ Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.⁴¹ Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.⁴² Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.⁴³ Many federal and state agencies also have confidentiality and breach notification requirements.⁴⁴ These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.⁴⁵

III. Conclusion

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

⁴⁰ State Bar of Mich. Op. RI-09 (1991).

⁴¹ National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.

⁴⁵ Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

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.”

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

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

CHAIR: Barbara S. Gillers, New York, NY ■ John M. Barkett, Miami, FL ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Michael H. Rubin, Baton Rouge, LA ■ Lynda Shely, Scottsdale, AZ ■ Elizabeth C. Tarbert, Tallahassee, FL ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

©2018 by the American Bar Association. All rights reserved.

Faculty

Christine E. Devine is a practitioner with the Law Office of Christine E. Devine, LLC in Medway, Mass., which she established in 2021. She has experience representing debtors and creditors in all aspects of bankruptcy and pre-bankruptcy workouts. Before establishing her firm, Ms. Devine was a partner for many years at a mid-sized law firm, where she chaired its Creditors' Rights, Bankruptcy and Reorganization Group. She worked on such complex matters as the representation of businesses in need of restructuring, trustees liquidating unique assets, and a wide range of businesses and individuals seeking cost-effective advice when encountering a distressed financial situation. Ms. Devine also has experience with commercial lending and has represented lenders and borrowers in all types of financing transactions, including general commercial financing, asset-based financing, real estate financing, participation agreements and intercreditor transactions. She is a frequent speaker on a range of bankruptcy-related and business topics, and became a Fellow in the American College of Bankruptcy in 2019. In 2020, *Lawdragon* recognized Ms. Devine as one of the "500 Leading U.S. Bankruptcy & Restructuring Lawyers," and in 2006, she was honored with the *Worcester Business Journal's* "40 under 40" award. She also was named a Massachusetts "Super Lawyer" by *Boston* magazine and *Law & Politics* from 2008-12 and from 2014-22. Ms. Devine teaches bankruptcy law classes at Suffolk University Law School and she is active as an alumna of the University of Massachusetts. She received her B.A. *cum laude* from the University of Massachusetts at Amherst in 1991 and her J.D. *cum laude* from Suffolk University Law School in 1994.

William K. Harrington is the U.S. Trustee for Regions 1 and 2 in New York, appointed to Region 1 on Nov. 8, 2010, and Region 2 on Nov. 26, 2013. Prior to his appointment, he was the Assistant U.S. Trustee for the District of Delaware and practiced bankruptcy and reorganization law at Duane Morris LLP. Prior to joining the Office of the U.S. Trustee, he practiced bankruptcy and reorganization law at Duane Morris LLP. Mr. Harrington is a member of the Boston, Delaware State and American Bar Associations, ABI and the Delaware Bankruptcy American Inn of Court. He received his undergraduate degree from the University of Pennsylvania and his J.D. from Villanova University School of Law.

Hon. Enrique S. Lamoutte is a U.S. Bankruptcy Judge for the District of Puerto Rico in San Juan, initially appointed in November 1986. He served as Chief Judge from 1986-98 and from 2009-18. He also serves as a judge for the U.S. Bankruptcy Appellate Panel for the First Circuit, over which he presided as Chief Judge. Judge Lamoutte is a Fellow in the American College of Bankruptcy. He previously clerked for U.S. District Judge Hernan G. Pesquera of the U.S. Bankruptcy Court for the District of Puerto Rico and was chief of the Civil Division of the U.S. Attorney's Office. He also is a retired colonel of the Puerto Rico Air National Guard. Judge Lamoutte graduated from Boston College in 1969 and received his J.D. from the University of Puerto Rico Law School in 1976.

Adam J. Ruttenberg is a partner at Beacon Law Group, LLC in Needham, Mass., where his principal areas of practice are bankruptcy litigation and business reorganization, representing debtors, creditors and bankruptcy trustees. He learned bankruptcy during almost five years at the Federal Deposit Insurance Corporation in an office responsible for the defaulted loans of approximately 40

failed banks. Mr. Ruttenberg was previously an attorney at Looney & Grossman LLP, Posternak Blankstein & Lund LLP and ArentFox Schiff LLP. Prior to attending law school, he worked in an actuarial program at John Hancock Mutual Life Insurance Company. Mr. Ruttenberg received his B.A. *summa cum laude* in mathematics from Yale University and his J.D. *magna cum laude* from Harvard Law School.