

WASHINGTON STATE BAR ASSOCIATION

Advisory Opinion: 2025-05

Year Issued: 2025

RPCs: 1.1, 1.3, 1.4, 1.5, 1.6, 3.3, 5.1, and 5.3

Subject: Artificial Intelligence-Enabled Tools in Law Practice

I. Introduction

Artificial intelligence has long been predicted to fundamentally reshape the legal profession. [n.1] This advisory opinion takes on a narrower topic: the ethical implications of using emerging artificial intelligence-enabled tools in law practice. [n. 2]

This advisory opinion uses the term “artificial intelligence”—AI—broadly to include “machine-based” AI that has existed for several years and focuses on making predictions or recommendations [n. 3], more recent “generative” AI that is trained to create new data and make related decisions [n. 4], rising forms of such as agentic AI that function as an agent for the user, and future forms such as autonomous AI that may function with a substantial degree of independence. [n. 5] “Artificial intelligence-enabled tools”—AI tools—in turn, refers broadly to software/hardware products and services. [n. 6, 7] Some are new standalone products, such as web or device-based “apps,” while others are products familiar to lawyers in daily practice that incorporate AI, such as legal research services. We have intentionally not attempted to focus on either specific products or narrow definitions in recognition that the technology is evolving rapidly. Rather, as noted, we have opted for broad considerations and general definitions in an effort to provide useful guidance over time going forward in a landscape likely poised for continual evolution.

AI tools presently used in or entering law practice [n. 8] encompass three diverse categories. First, some are open-source consumer products available to a wide spectrum of users that may be used in law practice. [n. 9] Second, others are products specifically tailored to law practice or other business users that include contractual assurances of confidentiality, similar to those commonly offered by commercial electronic communication and data storage providers. [n. 10] Third, emerging AI developments, while difficult to predict precisely, offer services that augment or possibly replace operating procedures and functions that law firms currently employ. [n. 11] Although the underlying duties are the same with all these categories, the practical analysis can differ.

This Advisory Opinion addresses seven duties under the Washington RPCs when using AI tools in law practice: (1) competence under RPC 1.1; (2) diligence under RPC 1.3; (3)

confidentiality under RPC 1.6; (4) communication under RPC 1.4; (5) candor toward tribunals under RPC 3.3; (6) supervision of other lawyers and nonlawyers under, respectively, RPCs 5.1 and 5.3; and (7) billing for their use consistent with RPC 1.5.

By discussing these areas, we do not suggest that these are the only topics that are or may become relevant to lawyers' use of AI tools. Rather, these are simply some of the more commonly encountered sets of issues to date. [n. 12] Similarly, for each area addressed, we have included illustrations. By offering these examples, we do not suggest that they are the only ways that such issues can arise. Further, by focusing on the topics selected, we also do not suggest that other law-related areas will not be impacted by AI. Finally, we have not evaluated substantive law beyond the RPCs—such as copyright and general data security law—that intersect with AI but are beyond the charge of our Committee.

Finally, our intent with the present advisory opinion is to provide broad guidance about general issues. We readily acknowledge and anticipate that specific practice areas and issues may warrant future advisory opinions tailored to those areas or issues as circumstances warrant.

II. Analysis

A. **Duty of Competence**

Lawyers must understand the technology they use in law practice.

RPC 1.1 states the duty of competence:

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

Comment 8 to RPC 1.1 explains that the duty of competence includes understanding technology used in law practice sufficiently to use it consistent with a lawyer's duties under the RPCs:

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**[.] [n. 13] (Emphasis added.)

In some instances, the use of technology in law practice is required—such as electronic filing mandated by court rules. [n. 14] In others, the use of technology may be a matter of personal choice or practical imperative—such as electronic documents with embedded metadata. [n. 15] Regardless of whether the use of a particular technology is required or is by choice, a lawyer using technology in law practice is obliged to do so competently. [n. 16] An author speaking of law practice technology generally neatly captured the practical import of the duty of competence in this regard:

Competence does not mean perfection, expertise, or paranoia. It does not mean that lawyers must now become early adopters, anxious to discover, purchase, and learn every possible new piece of legal tech. But it does require a baseline understanding of, and reasonable proficiency in, the technology at hand. [n. 17]

With AI-enabled general consumer products used in law practice, a lawyer must understand them sufficiently to use them consistent with the lawyer's duties under the RPCs. In a widely reported decision from New York, for example, a lawyer used a consumer-oriented AI-enabled web application to produce a brief that included citations to non-existent cases that the lawyer then filed in federal court without first checking them. [n. 18] When the court discovered the non-existent citations, the lawyer claimed a lack of understanding of how the application worked. [n. 19] The court sanctioned the lawyer nonetheless. [n. 20] Similarly, the ABA in Formal Opinion 498 (2021) noted that some "smart speakers" used as "virtual assistants" have default settings in which they "listen" for commands and may, therefore, allow their vendors to overhear confidential communications. [n. 21] ABA Formal Opinion 498 recommended that lawyers disable this feature if they use them in law practice. [n. 22] Although the RPCs do not prohibit the use of consumer-oriented AI-enabled products in law practice, lawyers must be sensitive to the fact that they may include features that must be understood and, if necessary, modified to make them compatible with law practice. In other instances where protection of client confidential information cannot be reasonably assured, lawyers should not use consumer-oriented AI tools.

With AI tools that are tailored to law practice and similar settings, a lawyer must understand them sufficiently to use them consistent with the lawyer's duties under the RPCs. With AI tools tailored to law practice, appropriate use of these products often (but not exclusively) turns on their contractual assurances of confidentiality consistent with lawyers' duties under RPC 1.6. Lawyers should understand the contractual terms of use and keep abreast of updated terms or privacy notifications from the vendor. In other words, it is not sufficient to simply note that an AI vendor offers a contractual assurance of confidentiality; rather, the terms must meet a lawyer's duty of confidentiality under RPC 1.6. WSBA Advisory Opinion 2215 (2012) discussed contractual terms of use in the analogous setting of cloud-based electronic file storage as part of a lawyer's duty of competence under RPC 1.1. [n. 23] While not an exclusive list, Advisory Opinion 2215 suggested that lawyers evaluate a vendor's contractual assurances in the context of overall industry practice, the vendor's record of meeting those obligations, and how information is handled by the vendor. Advisory Opinion 2215 also stressed that because technology changes over time, a lawyer's review cannot be static and must be revisited at appropriate intervals to give continued reasonable assurance that the product or service involved is still meeting standards compatible with those applicable to law practice. [n. 24] Advisory Opinion 2215 further notes that if particular nuances are beyond the lawyer's training and experience to evaluate, the lawyer should seek appropriate technical assistance in evaluating the vendor. We think that the general guidelines outlined in Advisory Opinion 2215 apply with equal measure to lawyers evaluating and using AI tools—whether standalone or incorporated into products commonly used in law practice.

At the same time, given the breadth of potential uses of AI tools in law practice, lawyers will also need to assess whether a particular tool is suitable for a given task and to evaluate its technical attributes in that regard. Depending on the circumstances, that may include an assessment of how the tool was trained and whether the training data may influence its results. In short, lawyers are responsible for the selection of particular tools used to carry out a representation and the lawyer—not the tool—is ultimately responsible for the work concerned. [n. 25.]

Whether considering products familiar to law practice that incorporate AI or new tools that promise to augment or replace existing operating procedures and functions, [n. 26] lawyers using them need to understand how they work so that they will be used consistent with the lawyer's duty of competence. [n. 27] Although the New York case noted earlier was an extreme example, it also underscored that lawyers remain ultimately responsible for their work under RPC 1.1—whether aided by AI tools or not.

Illustration

Amanda, a junior associate at a mid-sized law firm, is assigned a complex litigation case. Feeling overwhelmed by the volume of documents and tight deadlines, she decides to use a newly released AI legal research tool to assist with her work.

The AI tool that Amanda relied on is marketed as a cutting-edge AI product that can analyze vast amounts of legal documents, extract key information, and even draft legal memos. The product's website claims it can revolutionize legal research and writing.

Amanda's Actions

1. Without reasonably investigating the AI tool's capabilities and limitations, Amanda inputs sensitive client information and case details into the system.
2. She relies heavily on the AI tool to conduct legal research, accepting its findings without independently verifying the accuracy or relevance of the cited cases.
3. Amanda uses the AI tool to draft a crucial motion, making only minor edits to the AI-generated text before submitting it to the partner for review.
4. When the partner asks about her research methodology, Amanda simply states that she used advanced AI technology without explaining the specific process or her level of oversight.

Competence (RPC 1.1):

Amanda's actions implicate the duty of competence by:

- Failing to understand the limitations and potential risks of the AI tool
- Not critically analyzing the AI-generated output for accuracy and relevance.
- Relying on AI without exercising independent professional judgment.

B. Duty of Diligence

An AI tool that promises more efficiency must still be used competently.

RPC 1.3, in turn, outlines the duty of diligence:

A lawyer shall act with reasonable diligence and promptness in representing a client.

Although diligence focuses largely on handling a client's work with the attentiveness reasonably appropriate to the task involved, Comment 2 to RPC 1.3 notes that diligence is closely tethered to competence. In other words, to the extent an AI tool promises to make handling a task more efficient, a lawyer must still use it with the requisite technical competence. In *People v. Crabill*, 2023 WL 8111898 (Colo. Nov. 22, 2023) (unpublished), for example, a Colorado lawyer failed to act with reasonable diligence by using an AI tool to write a motion without verifying the accuracy of the citations the AI tool generated. The lawyer then filed a brief containing fictitious citations that were later discovered by the trial judge. The lawyer was disciplined under Colorado's analogous version of RPC 1.3 (and its similar version of RPC 1.1).

Illustration

See previous hypothetical.

Diligence (RPC 1.3):

Amanda's actions implicate the duty of diligence by:

- Not thoroughly reviewing and scrutinizing the AI-generated motion for legal and factual soundness.
- Failing to independently verify the cases and legal arguments presented by the AI tool.

The consequences of Amanda's actions can have a devastating impact on the case as follows:

1. The motion may contain inaccuracies, irrelevant citations, or even non-existent cases, potentially harming the client's case.
2. Amanda's lack of understanding of the AI tool's functionality could lead to inadvertent disclosure of confidential client information
3. If the court or opposing counsel discovers the heavy reliance on AI without proper oversight, it could damage the firm's reputation and potentially lead to sanctions.
4. Amanda's supervising attorney might also face ethical violations for inadequate supervision under RPC 5.1.

This example underscores the importance of lawyers maintaining their professional responsibilities even when using advanced AI tools. While AI can enhance efficiency, it cannot replace the critical thinking, judgment, and ethical obligations of a competent and diligent attorney. In short, lawyers cannot cede either their professional judgment or their responsibility for work to AI tools.

C. Duty of Confidentiality

Confidentiality embraces both information shared with an AI tool and how it is used.

Subject to specific exceptions, Washington RPC 1.6(a) states the duty of confidentiality:

A lawyer shall not reveal information relating to the representation of a client[.]

Washington RPC 1.6(c), in turn, outlines a lawyer's duty to take reasonable steps to protect client confidentiality:

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. [n. 28]

Comments 18 and 19 to RPC 1.6 weave together the duties of competence and confidentiality under the subtitle "Acting Competently to Preserve Confidentiality" and speak to these duties when using technology:

[18] 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 RPC 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. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by

making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forgo security measures that would otherwise be required by this rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see RPC 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's 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. 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules.

Although the duty of confidentiality remains the same, its practical import can vary depending on whether an AI-enabled product is developed primarily for consumers or is tailored to business and professional settings that include contractual assurances of confidentiality.

Some AI-enabled consumer products don't include contractual assurances of confidentiality thereby posing an unreasonable risk to confidential client information. In the New York sanctions decision discussed earlier, for example, the lawyer using the AI-enabled web application entered an increasingly specific series of prompts that revealed detailed client information—notwithstanding a disclaimer on the product concerned that data entered would not be kept confidential. [n. 29] The sanction was entered based on the non-existent cases the application generated and the lawyer used without checking their accuracy. Entering identifiable client confidential information into a non-confidential product, however, raises serious concerns under RPC 1.6. For example, lawyers may believe that entering a search in a public system using the “incognito” setting will be safe for their search—but it may not completely preserve confidentiality.

The duty of confidentiality under RPC 1.6 is broad—defined as “information related to the representation of a client” and extending beyond privilege and work product standing alone. [n. ³⁰] Moreover, a lawyer need not specifically intend to reveal confidential information to find a violation of RPC 1.6 if the lawyer intended the act that did, in fact, reveal the information. [n. ³¹] For example, as discussed earlier, ABA Formal Opinion 498 noted that using “smart speakers” with their “listening” function enabled may violate a lawyer's duty to protect confidential information. Similarly, lawyers should not share client confidential information with an AI-enabled product without verifying that the product will protect their client's confidentiality consistent with RPC 1.6.

Commercial AI tools that include contractual assurances of confidentiality should be evaluated using the general factors outlined earlier from Advisory Opinion 2215. [n. 32] In particular, the contractual terms should be examined to determine if the vendor uses the data involved for any other purpose (such as training the AI tool involved) and, if so, whether those purposes are compatible with the duty of confidentiality. [n. 33] Further, as reflected in Comments 18 and 19 to RPC 1.6 quoted above, and as discussed in Section D below, the sensitivity of the information involved in a particular representation may necessitate consultation with the client and, in some instances, obtaining the client's informed consent under RPC 1.6(a) before using an AI tool. [n. 34] Again as reflected in Comments 18 and 19 to RPC 1.6, clients may direct lawyers to refrain from using particular AI tools in some circumstances or may place other limits on such use.

Reflecting the intersecting duties of competence and confidentiality discussed in Comments 18 and 19 to RPC 1.6, lawyers are responsible for understanding AI tools sufficiently to protect client confidentiality in their actual use. [n. 35] For example, lawyers must understand end-user agreements and privacy policies that impact confidentiality. Similarly, lawyers using “chat bots” to assist with client intake by gathering preliminary information, should consider the use of appropriate disclaimers of an attorney-client relationship until expressly formed with the lawyer or law firm and related explanations on whether prospective clients may—or may not—supply preliminary information with an assurance of confidentiality. [n. 36] By using this example, we do not foreclose others. Rather, regardless of the product or service—whether existing or future—the duties of competence and confidentiality ultimately remain the lawyer's—not the product manufacturer or the service provider.

Illustration

Frank, a criminal defense attorney is hired on a complex case for a high-profile client. Feeling overwhelmed by the volume of discovery and tight deadlines, Frank decides to use a popular public-facing generative AI tool, such as ChatGPT, to help him draft a legal memo to the court. Frank inputs specific details about the case [n. 37] into the AI tool, including:

1. The client's name and identifying information
2. Confidential case strategies discussed with the client
3. Details of plea negotiations
4. Privileged communications between the client and the lawyer and paralegals

By entering this confidential information into a public AI platform, Frank's actions implicate the duty of confidentiality in several ways:

Unauthorized disclosure: The AI tool's employees may have access to the chat history, potentially exposing privileged information to unauthorized third parties

Data retention and usage: The AI platform may store and use the inputted information to train its model, making the confidential data potentially accessible to future users

Security risks: Public-facing AI tools may not have adequate security measures to protect sensitive legal information from cyber threats or data breaches.

Waiver of attorney-client privilege: By sharing privileged communications with the AI tool, Frank may inadvertently waive the attorney-client privilege, making those communications potentially discoverable by opposing counsel

Frank's actions implicate RPC 1.6, which requires lawyers to maintain client confidentiality.

Lawyers should thoroughly vet AI platforms for security and privacy measures and avoid inputting any sensitive or privileged information into public-facing AI tools. The next section addresses the issue of client consent.

D. Duty of Communication

Communication about AI tools will vary with the tool and the client.

RPC 1.4 outlines a lawyer's duty of communication. Although the rule is multi-faceted, two elements in particular potentially bear on a lawyer's use of AI tools.

First, RPC 1.4(a)(2) requires a lawyer to "reasonably consult with the client about the means by which the client's objectives are to be accomplished[.]"

Second, RPC 1.4(b) requires "[a] lawyer . . . [to] . . . explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the matter."

Echoing the analysis in the preceding section on confidentiality, in some instances, no specific discussion of AI tools may be required when, for example, they are tailored to law practice and offer contractual assurances of confidentiality consistent with RPC 1.6. In others, however, even if they do not require the client's informed consent under RPC 1.6, a lawyer's use of AI tools may nonetheless be required to conform to specific client objectives, requests, or preferences. ABA Formal Opinion 512 (2024), which surveys AI issues from a national perspective, concluded (and we agree) that circumstances will dictate the extent and nature of the communication reasonably required:

It is not possible to catalogue every situation in which lawyers must inform clients about their use of . . . [AI tools]. Again, lawyers should consider whether the specific circumstances warrant client consultation about the use of a . . . [AI] tool, including the client's needs and expectations, the scope of the representation, and the sensitivity of the information involved. [n. 38]

ABA Formal Opinion 512 notes (at 9)—and again, we concur—that if circumstances warrant discussion with the client about the use of AI tools (whether they rise to the level of informed consent under RPC 1.6 or not), an engagement agreement is a logical place to memorialize those discussions, any related instructions from the client, and, if applicable, the client's informed consent.

Illustration

Here's an example of how a lawyer can violate the duty of communication when using an AI product without obtaining informed consent:

Lola, a personal injury attorney, decides to exclusively use a new AI-powered legal research and drafting tool that her firm purchased to assist with her cases. She uses this tool from the inception of the case – which included drafting the initial demand letter to later developing legal memos and briefs in preparation for trial. The AI tool has been trained and tested by the law firm and most of the time produces consistent results.

Lola is able to complete her cases in a fraction of the time and has become complacent checking the results of the AI tool given the success in past cases.

Lola is hired by Jeremy in a medical malpractice case. Lola uses the same contract for legal services in Jeremy's case as she has used for years. This contract does not have a separate provision for the client to give informed consent for use of an AI product.

Lola also fails to orally communicate her use of the AI tool to her client. Lola then uses the AI product on the case, inserting confidential information into the system and extracting legal documents for use in the case.

While there may be multiple ethical issues, Lola's actions implicate the duty of communication in the following ways:

1. **Failure to disclose AI usage:** Lola does not inform Jeremy that she is using an AI products to conduct legal research and draft documents for his case.
2. **Lack of informed consent:** Lola fails to obtain Jeremy's approval before inputting his confidential information into the AI system.
3. **Inadequate explanation of risks:** Lola does not discuss the potential risks and limitations of using an AI product with Jeremy, such as data privacy concerns or the possibility of AI-generated errors.
4. **Omission of available alternatives:** Lola neglects to explain the reasonably available alternatives to using AI in Jeremy's case, preventing him from making an informed decision.
5. **Non-disclosure of AI's role:** When presenting legal strategies or documents to Jeremy, Lola does not mention that they were partially generated or influenced by an AI product.

This example underscores the importance of communication. RPC 1.4 require lawyers to reasonably consult with clients about the means used to accomplish their objectives. By failing to communicate her use of AI and obtain informed consent, Lola deprives Jeremy of the opportunity to make an informed decision about his representation and potentially exposes his confidential information to unauthorized disclosure.

E. Candor Toward the Tribunal

Lawyers are responsible for the accuracy of their court filings.

RPC 3.3 outlines a lawyer's duty of candor toward a tribunal. The term "tribunal," in turn, is defined broadly by RPC 1.0A(m) to include both courts and other "adjudicative" forums such as arbitrations and administrative agency proceedings.

Of particular relevance to the present topic, RPC 3.3(a)(1) prohibits a lawyer from making "a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer[.]" In *People v. Crabill*, *supra*, 2023 WL 8111898 (Colo. Nov. 22, 2023) (unpublished), for example, the Colorado lawyer who used an AI tool in preparing a motion failed to inform the court concerned when the lawyer discovered that the AI tool had generated fictitious citations that the lawyer had not verified before filing the motion. The lawyer was also disciplined under Colorado's analogous version of RPC 3.3(a)(1). [n. 39]

Similarly, a lawyer is also obliged generally under RPC 3.3(c) to alert the court to material evidence that the lawyer has discovered is false. In *Kohls v. Ellison*, 2025 WL 66514 (D. Minn. Jan. 10, 2025) (unpublished), for example, the Minnesota Attorney General informed the court when he learned that an expert declaration his office had submitted included citations to non-existent academic articles generated by an AI tool. The court struck the declaration involved. [n. 40]

Illustration

Attorney Adam represents a client on an appeal in federal court. Pressed for time and overwhelmed by the volume of research required, Adam decides to use a generative AI tool to help draft a key motion. The AI generates several persuasive arguments, complete with case citations.

Adam incorporates the AI-generated content into his motion without thoroughly verifying the citations or arguments. He submits the motion to the court without further review.

During oral arguments, the opposing counsel points out that two of the key cases cited in Adam's motion do not exist. The judge, unable to locate these cases, asks Adam to explain. Adam admits to using an AI tool but insists he believed the cases were real.

In this scenario, Adam's actions implicate the ethical rule of candor to the tribunal in several ways:

1. He submits false information to the court by including non-existent cases and fabricated arguments.
2. He fails to verify the accuracy of the AI-generated content before submitting it to the court.
3. When confronted, he does not immediately correct the false information, instead attempting to defend its validity.

This example shows the importance of lawyers understanding AI limitations, critically reviewing AI-generated content, and maintaining their ethical obligations when using such technology in legal practice. Adam's actions could result in sanctions and damage to his reputation.

F. Duty of Supervision

Those using AI tools must receive adequate training and supervision.

RPCs 5.1 and 5.3 [n. 41] address, respectively, a lawyer's duty to supervise other lawyers and nonlawyers. These duties extend to both lawyers and nonlawyers directly employed by a law firm or legal department, [n. 42] and independent contractors and vendors assisting a lawyer with a client's work. [n. 43]

In the context of AI tools, the duty of supervision has two primary aspects.

First, lawyers who supervise others—whether as a part of firm management or through direct supervision—have a responsibility to train lawyers and nonlawyers in the appropriate use of AI tools so they will be used in a manner consistent with the duties of competence and confidentiality discussed above.

Second, lawyers working with vendors supplying AI tools have a duty to evaluate the contractual assurances and other technical safeguards included in a particular product to ensure that its use is also consistent with the duties of competence and confidentiality as noted earlier.

Illustration

Anne, a senior partner at a large law firm, decides to implement a new AI-powered legal research tool across the firm. The firm's IT department researched an AI tool that would provide

protections of client confidentiality and utilize a system where it did not train on outside data.

Anne, excited about potential efficiency on cases, quickly rolled out the software to all associates and paralegals, providing only a brief email introduction on its basic functions. Anne left a more thorough training on the product up to the individual users.

Anne assigns a complex divorce case to Gabe. There are strict time limitations in place. Anne encourages Gabe to use the new AI tool. Gabe inputs some case details and asks the AI to generate arguments and find supporting case law. Without thoroughly reviewing the AI-generated content, Gabe incorporates it into the motion and submits it to Anne for final approval.

Anne, busy with a time-consuming trial – put trust into both the AI tool and Gabe's work. She gives the motion a cursory glance before filing it with the court. During the hearing, the judge points out that several key cases cited in the motion that are misquoted. Upon investigation, it's revealed that the AI tool had "hallucinated" these cases and citations.

In this example, Anne's actions implicate the duty of supervision in several ways:

1. **Inadequate training:** Anne failed to provide proper training on the ethical use and limitations of the AI tool.
2. **Clear AI use policies:** Anne did not establish clear guidelines for the use of AI in legal work, including the need for human verification. It is best practice for the firm to have an AI use policy handbook as well as regular training for employees who utilize the product.
3. **Lack of proper review of the motion:** Anne did not adequately review Gabe's work or ensure that he had properly vetted the AI-generated content.
4. **Too much reliance on technology:** By trusting the AI tool without question, Anne delegated her professional judgment to the AI, which is a violation of ethical standards.

This hypothetical highlights the need for comprehensive training, clear policies, and maintaining human oversight and professional judgment when using AI in legal work.

G. Duties under RPC 1.5

Billing for the use of AI tools must be reasonable.

RPC 1.5(a) prohibits a lawyer from making an agreement for, charging, or collecting an unreasonable fee or an unreasonable amount for expenses. RPC 1.5(b), in turn, requires that a lawyer explain the basis of fees and expenses at the outset of a representation and later if there is a modification to either. Comment 1 to RPC 1.5 explains further for expenses that "[a] lawyer may seek reimbursement for the cost of services performed in-house, such as copying, or for other expenses incurred in-house, such as telephone charges, either by charging a reasonable amount to which the client has agreed in advance or by charging an amount that reflects the cost incurred by the lawyer." [n. 44] Whether and how a lawyer or law firm may charge for the use of AI tools will vary with the circumstances and the lawyer or law firm's agreement with the clients concerned. Some, for example, may simply absorb those costs as overhead that is reflected in the firm's fee structure. Others, by contrast, may bill them separately as an expense. Regardless, any method of recouping the cost of AI tools must comply with RPC 1.5.

Further, AI tools may make some billable tasks more efficient. While lawyers may charge for time spent using AI tools—for example, creating appropriate prompts analogous to creating search terms for more traditional legal research programs—they may not charge for the "time saved" under RPC 1.5(a). In the analogous context of legal research, courts have noted that time

spent using computer-aided legal research is potentially recoverable (depending on the fee recovery statute or rule involved) because “[p]roperly utilized, it saves the client attorney fees which would otherwise be incurred for more time-consuming methods of legal research.” [n. 45]

Illustration

Maria, a lawyer at a small busy law firm purchased a sophisticated AI-powered legal research and document drafting tool for her practice. The AI tool was expensive, and Maria wants to pass along some of this expense to her clients for use in their cases.

Maria decides to use the AI tool on a simple case whereby she is reviewing and analyzing the contract. Maria then uses the AI tool which analyzes the contract and generates a comprehensive report with suggested revisions. The entire process, including Maria's review of the AI-generated content, takes only 2 hours.

However, Maria decides to bill her client for 10 hours of work at her usual hourly rate, reasoning that the AI tool's efficiency shouldn't reduce her billable hours. She justifies this by thinking about the time it would have taken her to do the work manually and the value provided to the client.

Maria's actions implicate RPC1.5 in several ways:

1. **Unreasonable fee:** By billing for 10 hours when the work only took 2 hours, Maria is charging an unreasonable fee that doesn't reflect the actual time spent on the task.
2. **Overhead cost:** Maria cannot pass on the cost of her overhead expenses to the client, without their informed consent in the use of the product. If the product costs to use it each time, then Maria should inform the client and get their consent to use this product in their case.
3. **Misrepresentation:** Maria is essentially misrepresenting the amount of time spent on the work, which violates the ethical obligation of honesty and transparency in billing practices.

To comply with Rule 1.5, Maria should instead:

1. Bill only for the actual time spent (2 hours) on the task, including the time used to review and refine the AI-generated content.
2. Consider adjusting her fee structure to reflect the value provided rather than time spent, such as implementing alternative fee arrangements.
3. Disclose the use of AI tools to the client and explain how it affects billing, ensuring transparency in the fee agreement.
4. Potentially bill separately for the cost of using the AI tool as a reasonable expense, if agreed upon with the client in advance.

By following these guidelines, Maria would maintain ethical billing practices while leveraging AI technology to benefit both her practice and her clients.

III. Conclusion

AI tools will undoubtedly continue to evolve and become more commonplace in daily law practice. Although they can assist lawyers in delivering legal services, they do not relieve lawyers of the core duties discussed in this advisory opinion.

-
1. See generally Anthony E. Davis, *The Future of Law Firms (and Lawyers) in the Age of Artificial Intelligence*, 27 No. 1 Prof. Lawyer 3 (2020).
 2. This opinion does not address ethical questions encountered by lawyers who may be embedded with software development teams or otherwise advising corporations, vendors, or venture capital funds who seek to develop or promote commercial AI-enabled products or features.
 3. 15 U.S.C. § 9401(3) (codifying National Artificial Intelligence Act of 2020 and defining AI as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.”).
 4. “Generative AI can be thought of as a machine-learning model that is trained to create new data, rather than making a prediction about a specific dataset. A generative AI system is one that learns to generate more objects that look like the data it was trained on.” <https://news.mit.edu/2023/explained-generative-ai-1109>. By using the term “generative AI,” we do not mean to limit the guidance offered in this opinion solely to that technology. Rather, we anticipate that AI will continue to evolve.
 5. See generally Chanley T. Howell and Alexander J. Liederman, “The Intersection of Agentic AI and Emerging Legal Frameworks,” National Law Review, Dec. 19, 2024 (available at www.natlawreview.com); Catherine Sanders Reach, “The Emergence of Agentic AI,” ABA Law Practice Magazine, July 3, 2025 (available at www.americanbar.org).
 6. For simplicity, this advisory opinion uses the term “products” broadly to reflect hardware, software, and associated services.
 7. See generally Daniel W. Linna Jr. and Wendy J. Muchman, *Ethical Obligations to Protect Client Data When Building Artificial Intelligence Tools: Wigmore Meets AI*, 27 No. 1 Prof. Lawyer 27 (2020).
 8. We acknowledge that the observations in this advisory opinion are inherently limited to present use of AI tools in a rapidly developing area. ABA Formal Opinion 512 (2024), which surveys AI issues in law practice from a national perspective, put it this way (at 2): “AI tools are a moving target—indeed a *rapidly* moving target—in the sense that their precise features and utility to law practice area quickly changing and will continue to change in ways that may be difficult or impossible to anticipate.” We have intentionally sought to focus our analysis, therefore, on core duties rather than specific products.
 9. See, e.g., *Mata v. Avianca, Inc.*, 678 F. Supp.3d 443 (S.D.N.Y. 2023) (web-based consumer application); ABA Formal Op. 498 at 6 (2021) (smart speakers).
 10. See, e.g., ABA Formal Op. 477R (electronic communication, data transmission and storage); WSBA Advisory Op. 2215 (2012) (cloud storage of electronic files). As

discussed further, because vendor terms and the technological environment change, lawyers must periodically reassess the contractual assurances provided by vendors to evaluate whether they remain consistent with lawyers' duties.

11. See, e.g., ABA Formal Op. 506 (2023) at 2 (noting that law firms increasingly use technology to augment human interactions in preliminary client intake tasks).

12. Other recent studies, for example, have also touched on potential unauthorized practice of law and lawyer marketing issues. See New York State Bar Association Task Force on Artificial Intelligence, Report and Recommendations at 31 (Apr. 6, 2024) (surveying potential unauthorized practice issues); Florida Bar Ethics. Op. 24-1 at 7 (Jan. 19, 2024) (surveying potential lawyer marketing issues).

13. Comment 8 was amended to include the reference to technological competence in 2016. See Washington Supreme Court Order 25700-A-1146 (June 2, 2016). The Washington amendment followed a similar amendment to the corresponding ABA Model Rule comment in 2012. See ABA, *A Legislative History: The Development of the ABA Model Rules of Professional Conduct, 1982-2013* (ABA Legislative History) at 42-43 (2013). The ABA amendment was developed by the ABA's Ethics 20/20 Commission and reflected the Commission's focus on, in relevant part, technology in law practice. *Id.*

14. See, e.g., U.S. District Court for the Western District of Washington LCR 5(d).

15. See, e.g., WSBA Advisory Op. 2216 (2012) (using electronic documents with embedded metadata); ABA Formal Op. 06-442 (2006) (same).

16. See, e.g., *In re Hilborn*, 22 D.B. Rptr. 102 (Or. 2008) (lawyer disciplined under Oregon RPC 1.1 for failure to understand mandatory federal court electronic filing technology); *Hur v. Lloyd & Williams, LLC*, 25 Wn. App.2d 644, 654 n.6, 523 P.3d 851 (2023) (noting the requirement of technological competence under RPC 1.1 when using electronic documents with embedded metadata).

17. Ivy B. Grey, *Exploring the Ethical Duties of Technology Competence, Part I*, ABA Law Technology Today, Mar. 8, 2017 (available on the ABA's web site).

18. *Mata v. Avianca, Inc.*, *supra*, 678 F. Supp.3d 443.

19. *Id.*

20. *Id.* Referring to this case in his 2023 Year-End Report on the Federal Judiciary (2023 Year-End Report), Chief Justice Roberts pithily described (at 6) not cite-checking cases to ensure their accuracy as “[a]lways a bad idea.”

21. ABA Formal Op. 498 at 6. See also Jan L. Jacobowitz, *Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers*, 4 Tex. A&M J. Prop. L. 407, 420-24 (2018) (discussing “smart speakers” used by lawyers as “virtual assistants”). These confidentiality issues have been accentuated with the

increasing norm of “remote work” where lawyers and staff are working from home and such consumer products may play both work and personal roles distinct from their use in a traditional “brick and mortar” law office. See ABA Formal Op. 498, *supra*, at 3 (discussing supervision in the virtual practice context); see *also* ABA Formal Op. 495 (2020) (remote work).

22. ABA Formal Op. 498 at 6.

23. By citing WSBA Advisory Opinion 2215, we do not imply that cloud computing and AI are equivalent technologies. For present purposes, however, they share the common trait of potentially holding client confidential information.

24. ABA Formal Opinion 477R includes a similar set of factors to evaluate vendors handling client confidential material at 9. An “appropriate interval” will necessarily vary with both the vendor (for example, a vendor affirmatively amends its terms of use) and technology (what is “state of the art” today may no longer be so in the future).

25. See, e.g., ABA Formal Op. 517 at 5-6 (2025) (discussing the use of AI tools in jury selection and making the point that the lawyer-user—not the AI tool—remains ultimately response for the work involved).

26. In his 2023 Year-End Report, Chief Justice Roberts noted (at 4) that before the U.S. Supreme Court bought its first photocopier in 1969, most internal memoranda were typed on carbon paper and duplicated on a hot-lead printing press.

27. Competent use also includes understanding and complying with any applicable court rules on AI.

28. RPC 1.6(c) was added in 2016. See Washington Supreme Court Order 25700-A-1146, *supra*. The Washington amendment followed a similar amendment to the ABA Model Rules in 2012 as a part of the ABA Ethics 20/20 Commission’s suggested amendments. See ABA Legislative History, *supra*, at 143-46.

29. See *Mata v. Avianca, Inc.*, *supra*, 678 F. Supp.3d at 457.

30. See Washington RPC 1.6, cmt. 3 (discussing the relationship between the confidentiality rule, attorney-client privilege and work product).

31. See *In re Cross*, 198 Wn.2d 806, 820, 500 P.3d 958 (2021).

32. See *also* ABA Formal Op. 477R, *supra*, at 9 (listing criteria similar to Washington Advisory Op. 2215).

33. See Texas State Bar Ethics Op. 705 at 4 (2025) (addressing the issue of potential vendor use of information).

34. See *also* RPCs 1.2(a) (lawyer consultation with clients on the means used to carry out a client's work), RPC 1.4 (communication with client). See *generally* ABA Formal Op. 08-451 (2008) (discussing outsourced legal and support services).

35. As discussed earlier, this includes both understanding them when acquired and monitoring changes in, for example, end-user agreements and privacy policies that impact confidentiality.

36. See ABA Formal Op. 506, *supra*, at 2 (use of technology to assist client intake); RPC 1.18 (duties to prospective clients); see *also* WSBA Advisory Op. 20280 (2006) (client intake through law firm web sites); *Barton v. U.S. District Court*, 410 F.3d 1104 (2005) (same).

37. Depending on the circumstances, court orders, discovery agreements between the parties, or other substantive legal restrictions may limit the information that can be shared with an AI tool.

38. ABA Formal Op. 512, *supra*, at 9.

39. If the procedural rules in a particular court require disclosure of a lawyer's use of AI tools in preparing submissions, then RPC 3.4(c) generally requires a lawyer to follow the rule.

40. Potential court sanctions for inaccurate citations and related issues are beyond the scope of this opinion. Courts have made plain, however, that a lawyer's risk in this regard is not limited to possible regulatory discipline. See *generally Park v. Kim*, 91 F.4th 610 (2d Cir. 2024) (discussing duties Fed. R. Civ. P. 11 in context of lawyer who used AI tool in preparing brief that generated fictitious citation).

41. RPC 5.3 is entitled "Responsibilities Regarding Nonlawyer Assistants." ABA Model Rule 5.3, by contrast, uses the word "Assistance" rather than "Assistants." The ABA version was changed from "assistants" to "assistance" in 2012 to reinforce that the rule applies to both nonlawyer employees of a law firm and nonlawyer independent contractors who are working with the firm. See ABA Legislative History at 604. Washington did not adopt this semantic change. Read in context, both rules refer to human nonlawyers—including vendors supplying services. See *generally LK Operating, LLC v. Collection Group, LLC*, 181 Wn.2d 48, 75-76, 331 P.3d 1147 (2014) (RPCs interpreted using principles of statutory construction). Purely technological "virtual assistants"—at least pending clarifying amendments to either the text or the comments of the rules concerned—are governed by a lawyer's duties of competence and confidentiality discussed earlier.

42. RPC 1.0A(c) defines "firm" broadly to include law firms, corporate and governmental law departments, and similar organizations. We use the term "firm" here in that broad sense.

43. See ABA Formal Ops. 08-451, *supra* (addressing outsourced legal and support services) and 477R, *supra* (discussing the use of outside vendors for electronic communication, data transmission and file storage). See *also* ABA Formal Op. 512, *supra*, at 11 (suggesting application of approaches used to vet other law practice technology for compliance with the duty of confidentiality to AI tools).

44. See *also* WSBA Advisory Op. 2120 (2006) (billing for expenses); ABA Formal Op. 93-379 (1993) (same).

45. *Absher Const. Co. v. Kent School Dist. No. 415*, 79 Wn. App. 841, 848, 917 P.2d 1086 (1995); *In re Guardianship of Hays*, 2013 WL 4607075 at *6 (Wn. App. Aug. 26, 2013) (unpublished) (citing *Absher* on this point); *Amkal v. Cingular Wireless, Inc.*, 2007 WL 9775545 at *3 (W.D. Wash. Sept. 7, 2007) (unpublished) (same).

Advisory Opinions are provided for the education of the Bar and reflect the opinion of the Committee on Professional Ethics (CPE) or its predecessors. Advisory Opinions are provided pursuant to the authorization granted by the Board of Governors, but are not individually approved by the Board and do not reflect the official position of the Bar association. Laws other than the Washington State Rules of Professional Conduct may apply to the inquiry. The Committee's answer does not include or opine about any other applicable law other than the meaning of the Rules of Professional Conduct.