Ethical Cloud and AI Vendor Selection for Criminal Defenders

2026

Maya Dimant | Jeff Sherr

Ethical Cloud and AI Vendor Selection for Criminal Defenders

This white paper provides a step-by-step framework for selecting, contracting with, and supervising any cloud or AI vendor that will touch confidential discovery, privileged work product, or client communications in a criminal defense setting. It is designed to be used by people making technology decisions within criminal defense settings.

Executive Summary

Public defenders are drowning in digital evidence: body-worn camera video, jail calls, surveillance footage, forensic extractions, and hours of recorded interviews. Human review alone can no longer keep up. Cloud platforms and AI tools are now functionally unavoidable to review, organize, search, summarize, and share this material.

That shift creates myriad ethical problems: privileged client information and defense work product now live on someone else's servers, often processed by someone else's AI. If those vendors reuse the data, give law enforcement indirect access, or delay telling you about a breach, you may be exposing clients in ways that violate your professional duties.

One critical ethical area of note is the risk of data co-mingling when a vendor simultaneously serves both defense and law enforcement customers. This creates a structural tension that can be difficult to resolve through contract terms alone.

There are ways to adopt technology ethically. Practitioners can demand contracts that:

- Preserve confidentiality and privilege
- Prevent AI vendors from using lawyers' uploaded files to improve (train) their AI systems
- Strictly segregate defense data from law enforcement customers
- Guarantee breach notice fast enough to notify clients
- Guarantee vendors will resist or appeal subpoenas/warrants on attorney's behalf
- Give counsel audit trails and full data export upon discontinuation of service

This paper gives you

Following this process will ensure a documented, defensible record to satisfy duties of confidentiality, competence, loyalty, supervision, and communication to clients.

Section 1

Application of Relevant Ethics Rules and Opinions

Application of Relevant Ethics Rules and Opinions

Making sound ethical decisions requires a careful review of the rules of professional conduct. Here is a selection of the applicable provisions and the opinions interpreting them.

1. Rule 1.1 – Competence

An attorney must provide competent representation, which now includes understanding 'the benefits and risks associated with relevant technology'.[1] Competence means the lawyer either:

> Understands how a tool works, what it does with client data, and what its limits are,
>
> **OR**
>
> Gets qualified help (internal IT, vendor security officer, outside consultant) to evaluate it. The ABA Model Rules suggest associating with another lawyer of established competence. ABA Formal Opinion 512 is more specific to AI, and allows obtaining help from Generative Artificial Intelligence [“GAI”] experts or others. The attorney must acquire a reasonable understanding of the capabilities and limitations of the specific GAI technology they use or draw on the expertise of others who can provide guidance about the relevant GAI tool’s functions and risks.[2]

In defining competency in this context, ABA Formal Opinion 512 (2024) notes that attorneys cannot rely on AI output blindly. The opinion elaborates, “[B]ecause GAI tools are subject to mistakes, lawyers’ uncritical reliance on content created by a GAI tool can result in inaccurate legal advice to clients or misleading representations to courts and third parties.” Counsel must therefore understand accuracy limits, hallucination risk, and confidentiality risk before using AI in client work.[3]

---

[1] Model Rules of Pro. Conduct r. 1.1 cmt. 8 (Am. Bar Ass’n).

[2] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 512, at 3 (2024). "Rather, lawyers must have a reasonable understanding of the capabilities and limitations of the specific GAI technology that the lawyer might use... or draw on the expertise of others[.]"

[3] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 512, at 5 (2024). (Because GAI tools are subject to mistakes, lawyers’ uncritical reliance on content created by a GAI tool can result in inaccurate legal advice to clients or misleading representations to courts and third parties”)(“A lawyer using GAI must be cognizant of the duty under Model Rule 1.6 to keep confidential all information relating to the representation of a client, ... Lawyers also must make ‘reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.’”)

2. Rule 1.4 – Communication

Counsel must provide the information and explanations reasonably necessary for the client to make informed decisions.[4]

In this context, ABA formal opinion 512 explains that if using AI meaningfully affects cost, strategy, or requires uploading highly sensitive client information into a third-party system, counsel must disclose use of the tool to the client and obtain their consent for use.[5]

— **Example Application:** Properly comporting with Rule 1.4 requires lawyers to keep abreast of shifting vendor terms to ensure competence in informing clients of material risks. Thus, counsel should be wary of vendors that want to change their privacy policies or security practices without notice: One service used by criminal defense attorneys has this in their terms - “We may revise and update these Terms of Use from time to time in our sole discretion. All changes are effective immediately when we post them, and apply to all access to and use of the Website thereafter. Your continued use of the Service constitutes acceptance of such changes. Check this page periodically for updates." This would allow a vendor to change what data is used for AI training or lower encryption standards overnight, which would put client data at risk without the attorney’s knowledge. The attorney would not be able to meaningfully convey risks to her client if she herself is not aware of them.

As applied to cybersecurity, ABA formal opinion 483 notes: If there is a material breach that compromises a current client’s confidential information or materially affects counsel’s ability to defend them, Rule 1.4 obligates the attorney to promptly tell that client what happened, what data was affected, and what they are doing about breach.[6] This is a diligence standard, meaning that best practice dictates that lawyers proactively develop an incident response plan to ensure their ability to promptly meet the ethical duty to notify.[7]

---

[4] Model Rules of Pro. Conduct r. 1.4(a)(3) & (b) (Am. Bar Ass’n). (requiring a lawyer to keep the client reasonably informed about the matter's status and explain matters necessary to permit the client to make informed decisions),

[5] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 512 at 7 (2024). "Lawyers should use professional judgment to determine, based upon the circumstances, whether disclosure of GAI tool use is necessary to comply with Rule 1.4.

[6] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 at 11 (2018). (“When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information, lawyers have a duty to notify clients of the breach.”)

[7] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 at 6 (2018). "Best practice dictates that a firm have a breach response plan in place with 'specific plans and procedures for responding to a data breach.'"

3. Rule 1.6 – Confidentiality

Counsel must not reveal information relating to the representation without consent.[8] Model Rule 1.6(c) adds that attorneys must make "reasonable efforts" to prevent unauthorized access or disclosure.[9]

In this context, suggested compliance looks like:

- Vetting vendors for confidentiality and breach handling.[10]
- Ensuring the vendor will not mine, resell, or train on counsel's privileged data.[11]
- Ensuring encryption, access control, and audit trails exist.[12]
- Responding to breaches: stopping the leak, mitigating harm, and notifying clients where ethically required.[13]

3a. 1.6 Breach Duties (ABA Formal Op. 483 & Rule 1.4)

Modern guidance clarifies what happens when something goes awry:

1. The attorney must act competently to contain the incident and stop further exposure of client data.[14]
2. Counsel must investigate what was accessed or exfiltrated.[15]

---

[8] Model Rules of Pro. Conduct r. 1.6(a) (Am. Bar Ass'n). (prohibiting a lawyer from revealing information relating to the representation without informed consent, unless impliedly authorized or permitted by the Rule).

[9] Model Rules of Pro. Conduct r. 1.6(c) (Am. Bar Ass'n). "(c) 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] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017). (listing required due diligence steps, including investigating the vendor's security policies and ensuring remediation of data breaches or security lapses) (Supervision: Rule 5.3).

[11] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512 at 6 (2024). "Lawyers must ensure that any client information entered into a GAI tool... is not used by the GAI provider for training its model or other purposes inconsistent with the lawyer's ethical obligations."

[12] N.C. State Bar, 2011 Formal Ethics Op. 6 (2012). ("The lawyer must ensure that the [cloud] provider uses technology and practices that protect against the risk of data loss, such as robust backup systems, and that the provider's data transmission and storage methods provide reasonable assurance of confidentiality, including the use of adequate encryption.").

[13] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 5 (2018). ("When a data breach or cyberattack has occurred, a lawyer must act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."); id. at 11 ("When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information, lawyers have a duty to notify clients of the breach.").

[14] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("Following a data breach, a lawyer must act reasonably and promptly to stop the breach and mitigate the damage.") (Competence: Rule 1.1)

[15] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("A lawyer must also ensure that the breach is remedied by investigating the cause of the breach and its extent, including the scope of any disclosure of confidential client information.") (Competence: Rule 1.1)

3. If a client's confidential information was materially exposed, and it impacts their case or counsel's ability to represent them, counsel must promptly inform the client, explain what was affected, and detail what they are doing about it (Rules 1.4 and 1.6).[16] Contractual notification requirements must be robust enough to enable the lawyer to promptly meet this ethical standard.[17]
4. Afterward, counsel must improve safeguards. The duty is ongoing, it cannot be satisfied simply by patching and moving on.[18]

— **Example Applications:** Distinguishing between vendors who treat your data as inside a vault versus those who treat it as a resource mine is critical. Be cautious of agreements that force counsel to waive privilege so that the vendor can use client files to build better products.

One current AI transcription service's Terms of Service state: "You authorize the Company to use such Machine Learning for testing, tuning, optimizing, validating, or otherwise enhancing the analytics, models, or algorithms underlying the System." Another similarly broad agreement notes that the vendor "reserves the right to utilize 'Client Content' in an aggregated and anonymized manner without restriction." These terms expose privileged case files to becoming training fodder for a commercial model that could be sold to anyone, including the prosecution. Relatedly, be mindful of language in a contract allowing the vendor to outsource your work: "[work product] may be rendered by... third parties selected by [Vendor] in [Vendor's] sole and absolute discretion." This leaves the attorney liable for a breach caused by a subcontractor they didn't know existed.

The most important confidentiality risk is preserving client data from law enforcement. Thus, it behooves attorneys to be especially cautious about contracts that give vendors wide discretion to cooperate with authorities. Note platform terms that allow disclosure "to law enforcement authorities as we reasonably feel is necessary" or "if we believe disclosure is necessary... to protect the safety of [Vendor], our customers, or others." These subjective standards allow private companies to divulge privileged client information and work product based on a "feeling" rather than a court order.

---

[16] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("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.") (Communication: Rule 1.4)

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The lawyer should have a remediation plan in place for prompt client notification.") (Diligence: Rule 1.3)

[18] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The duty of competence under Rule 1.1 requires the lawyer to take reasonable efforts to monitor and update security measures... to protect client confidential information.") (Competence: Rule 1.1)

Duty to Resist Compelled Disclosure: A lawyer ordered by a court to disclose client confidences must not comply until they have made every reasonable effort to appeal the order or have notified the client to give them an opportunity to challenge it.[19] Because vendors may be subject to court orders disclosing client information, defenders' contracts with those vendors must mandate that vendors immediately notify the attorney of any subpoena or warrant. Vendors must also agree to fight or delay disclosure until the attorney exhausts its appeal rights.[20] This non-delegable duty must be enforced through contract under Rule 5.3.[21]

— **Example Application:** To comply with the duty to resist compelled disclosure, counsel must be vigilant about vendor contracts that allow the vendor sole discretion in when to maintain confidentiality- note this actual contract example: "Vendor shall treat all Client Content as confidential, unless Vendor determines [it is necessary to disclose Client Content], in its sole and absolute discretion…for the health, safety or welfare of any individual." In this example, the vendor has the absolute power to determine when, why, and to whom client content could be disclosed, which is a grave risk.

4. Rule 1.7 – Conflicts of Interest

A material limitation conflict arises under *Model Rule 1.7(a)(2)* when "there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person, or by a personal interest of the lawyer." An attorney cannot let their duties to another party materially limit their loyalty to their client.[22] The duty of criminal defense lawyers to remain independent of political or judicial influence is paramount.[23]

In Formal Opinion 512, the ABA notes that if an AI vendor's data practices or commercial incentives could harm clients, the attorney must recognize and address that conflict before using the tool.[24]

---

[19] Model Rules of Pro. Conduct r. 1.6 cmt. 18 (Am. Bar Ass'n) ("The lawyer must assert all nonfrivolous claims that the order is not authorized by law or that the information sought is protected against disclosure by an applicable privilege or other law.") (Confidentiality: Rule 1.6)

[20] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 7 (2017) (requiring lawyers to ensure by contract that the vendor notifies the lawyer immediately upon receiving any subpoena or court order regarding the client's information) (Supervision: Rule 5.3)

[21] N.Y.C. Bar Ass'n, Formal Op. 2024-5, at 10 (2024) (stating that lawyers must exercise appropriate supervision under Rule 5.3 to ensure the GAI provider is contractually bound to preserve confidentiality and to notify the lawyer of any disclosure requests) (Supervision: Rule 5.3)

[22] Model Rules of Pro. Conduct r. 1.7(a)(2) (Am. Bar Ass'n). ("there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.")

[23] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-441 (2006). ("A lawyer who is employed full-time by a governmental entity to provide defense services to indigent clients has the same ethical obligations as any other lawyer[.]")

[24] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512 at 7-8 (2024). ("Lawyers must be alert to potential conflicts of interest that may arise from the use of a particular GAI tool. For example, if the GAI provider's data-handling practices or its commercial interests could adversely affect a client's interests, the lawyer must address the conflict before using the tool.")

Formal Opinion 512 also explains that inputting confidential information into self-learning AI systems is permissible with the client's informed consent.[25] However, in practice, obtaining comprehensive, fully informed consent from every indigent client across a mass representation practice to allow their data to be used by a third-party AI is beyond the capacity of most public defender and large criminal defense offices. Because of this impracticality, the lawyer must assess whether the conflict is consentable under Rule 1.7(b)(1) and (4).[26]

A vendor who is: serving law enforcement, and/or reuses defender data, and/or is financially dependent on the State potentially creates a structural conflict. It should be evaluated as a possible material limitation conflict under Rule 1.7(a)(2) because the vendor's divided business interests may temper the defender's ability to aggressively challenge the vendor's technology or security in litigation. It could also force defenders to prioritize adversarial customers over client loyalty.[27]

— **Example:** When a defense firm or organization depends on a technology vendor that also serves law-enforcement clients, the vendor's commercial and reputational interests may conflict with the defender's litigation posture. If the defender hesitates to challenge or expose flaws in the vendor's technology for fear of losing essential service, access, or favorable terms, that dependence creates a significant risk of materially limiting the lawyer's representation under Rule 1.7(a)(2).

When a vendor simultaneously serves local law enforcement/prosecutors and the defense on related evidence/AI systems, decision makers should closely evaluate whether a Rule 1.7(a)(2) material-limitation conflict exists, considering these factors:[28]

1. **Lack of agency in selecting vendor:** Funding authorities or administrative agencies may expect/force defenders to choose specific vendors without the autonomy to vet and evaluate in order to ensure alignment with ethical rules.[29]

---

[25] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512, at 6 (2024). "Before lawyers input information relating to the representation of a client into a GAI tool, they must evaluate the risks that the information will be disclosed to or accessed by others outside the firm."

[26] Model Rules of Pro. Conduct r. 1.7(b)(1) & (4) (Am. Bar Ass'n). ("(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if: (1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client; and (4) each affected client gives informed consent, confirmed in writing.")

[27] Model Rules of Pro. Conduct r. 1.7 cmt. 8 (Am. Bar Ass'n). ("The critical questions are the likelihood that a difference in interests will eventuate and, if it does, whether it will materially interfere with the lawyer's independent professional judgment and foreclose courses of action that reasonably should be pursued on behalf of the client.")

[28] Model Rules of Pro. Conduct r. 1.7 cmt. 8 (Am. Bar Ass'n).

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451, at 3 (2008) ("A concurrent conflict of interest exists if ... there is a significant risk that the representation ... will be materially limited by the lawyer's responsibilities to ... a third person ...." ; "The critical questions are ... whether [it] will materially interfere with the lawyer's independent professional judgment ... ."), (Shared platforms used by both prosecutors and defenders create potential third-party or institutional conflicts that may materially limit independent professional judgment, triggering Rule 1.7 conflict analysis and disclosure.)

2. **Use of Shared AI systems or review staff:** The company uses the same artificial-intelligence tools or human reviewers for both law enforcement and defense customers—meaning the same people or systems could handle evidence from both sides.[30]
3. **Reuse of defense information for product development/improvement:** The company improves its software or trains its AI by using defense materials, case data, defense feature requests, or how defenders interact with the system—even if supposedly "de-identified."[31] This means law enforcement customers are using a product that improves based on integrating defender inputs, usage, and feedback.
4. **Vendor access to defense files or activity logs:** The company's employees can see activity records, file names, or usage data from the defender's workspace—even if they can't open the actual evidence. This could enable law enforcement customers to predict and prepare for strategic defense litigation choices.[32]
5. **No independent control over data security:** The defender office cannot control or hold its own encryption keys—meaning the vendor could technically access or turn over data if compelled.[33]
6. **No protection against retaliation or service cutoff:** The vendor provides no guarantee that it will continue service, support, or fair pricing if the defender's lawyers challenge the vendor's technology in litigation.[34]

5. Rule 5.3 – Supervision of Nonlawyers (Vendors)

ABA Formal Opinion 498 explains that vendors, outsourced transcription services, cloud platforms, and AI tools are all 'nonlawyer assistants.'[35]

---

[30] Model Rules of Pro. Conduct r. 1.7 cmt. 8 (Am. Bar Ass'n).

[31] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512, at 7-8 (2024) ("Lawyers must be alert to potential conflicts of interest that may arise from the use of a particular GAI tool. For example, if the GAI provider's data-handling practices or its commercial interests could adversely affect a client's interests, the lawyer must address the conflict before using the tool.") (Conflict of Interest: Rule 1.7).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 5-6 (2017) ("[In selecting a technology vendor,] the lawyer should consider ... what the provider's policies are for data retrieval and loss.") (Competence: Rule 1.1; Supervision: Rule 5.3).

[33] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 5-6 (2017)("The lawyer must undertake reasonable efforts to ensure that the provider's conduct is compatible with the professional obligations of the lawyer," including evaluating "how the provider stores and secures data" and "what the provider's policies are for data retrieval and loss.") (Competence: Rule 1.1; Supervision: Rule 5.3).

[34] Model Rules of Pro. Conduct r. 1.1 cmt. 8 & r. 5.3(b) (Am. Bar Ass'n 2024) ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of ... the benefits and risks associated with relevant technology." ; "A lawyer having direct supervisory authority over [a] nonlawyer shall make reasonable efforts to ensure that [their] conduct is compatible with the professional obligations of the lawyer."), (A lawyer must evaluate vendor reliability and continuity of service; contracts allowing unilateral termination or retaliation for litigation challenges undermine competence and supervisory duties.)

[35] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 498, at 2 (2021) ("Contractors... and third-party vendors for outsourcing... are 'nonlawyer assistants' or 'agents' within the meaning of Model Rule 5.3.") (Supervision: Rule 5.3)

The opinion stresses that counsel is responsible for proper supervision of remote staff, contractors, 'nonlawyer assistants,' and vendors to ensure they act in a manner compatible with all ethical obligations.[36] The primary mechanism for meeting this duty is the procurement contract.[37]

— **Example Application:** Companies often contract out specific services to third parties. Rule 5.3 makes it clear that attorneys are still responsible for the actions of those third parties. Accordingly, be wary of contracts that state: "The Company takes no responsibility and assumes no liability for any actions or omissions of such third party."

Taken together, these duties form the 'ethics spine' for technology procurement: confidentiality, competence, loyalty, supervision, client communication, and breach response are not optional—they are mandatory and reviewable.

[36] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 498, at 2 (2021) ("A lawyer who uses nonlawyer assistance... remains responsible for proper supervision of the nonlawyer... to ensure that they act in a manner compatible with the professional obligations of the lawyer.") (Supervision: Rule 5.3)

[37] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 6 (2017) (requiring lawyers to ensure, by contract, that the vendor adheres to confidentiality and security obligations commensurate with the lawyer's own duties under the Model Rules) (Supervision: Rule 5.3)

Section 2

Risk Domains to Evaluate Before Contracting with an AI/Cloud Vendor

Every potential vendor should be evaluated across seven risk domains. These domains will tie directly into the scorecard and the contract addendum.

A. Confidentiality / Privilege

Key questions:

- Does the vendor ever re-use defender data (audio, video, transcripts, notes, annotations) to train their models or other customers' models?
- Are they sharing infrastructure, databases, or staff with law enforcement customers?
- Is there any term that allows law enforcement or prosecution to access 'their own evidence' through the vendor in a way that backdoors into your work product?
- Is all data encrypted in transit and at rest? Who holds the keys?
- **Will the vendor contractually agree to resist or appeal judicial/governmental demands for disclosure?**
    - Will the vendor notify you before handing over data in response to a subpoena or warrant?

Ethics linkage: Model Rule 1.6 (confidentiality and reasonable efforts), ABA Opinions 477R, 498, 512, and modern breach guidance.

B. AI / Automated Analysis

Key questions:

- What AI models are touching the data—first-party models (built and run by the same vendor), or external providers like OpenAI/Google/etc.?
- Do third parties ever train on your client data or store snippets outside a secure enclave?
- Can you ensure that third party vendors will not train on your data, sell your data, or contribute your data to a dataset?
- Are AI-generated summaries flagged as potentially incomplete or biased, requiring human verification?

Ethics linkage: Rule 1.1 (competence with tech), Rule 1.6 (confidentiality), ABA 512 (AI must be supervised, outputs verified, and confidential data controlled).

C. Vendor Alignment / Conflict of Interest

Key questions:

- Who is the vendor's primary customer: prosecution/police, or defense?
  - Are they fundamentally a law-enforcement evidence management platform with a 'defense add-on'?
- Do they log, analyze, or monetize defender usage data in ways that could advantage law enforcement?
- Do they claim to be a neutral 'evidence hub' used by both sides?

Ethics linkage: Rule 1.7 (conflicts of interest—this domain poses the highest structural threat), Rule 5.3 (you must supervise vendors whose incentives might oppose your client's).

D. Access Controls, Audit Trails, and Least Privilege (every user or process should have only the minimum access necessary)

Key questions:

- Can you restrict who at the vendor can view content, except under a documented emergency protocol?
- Do you get tamper-proof audit logs showing who accessed what, when, and why?
- Can you pull those logs for litigation (Brady/Giglio challenges, chain-of-custody fights, suppression motions)?

Ethics linkage: Rule 5.3 (supervising nonlawyers), Model Rule 1.6 (limiting access), ABA 498 (oversight of remote/cloud practice).

E. Data Residency / Hosting Stack

Key questions:

- Where is the data physically stored? Which cloud (Google Cloud, AWS, Azure, etc.)?
- Is the data isolated in a CJIS-like locked project for defense, or in a shared SaaS bucket alongside police data?
- Will they notify you before adding new subprocessors?

Ethics linkage: Rule 1.6 (reasonable efforts to prevent unauthorized access) and Rule 5.3 (requiring subprocessors to follow confidentiality and security obligations).

F. Incident Response & Breach Duties

Key questions:

- If there's a breach, how fast will they notify you? (Contractual obligation must enable lawyer's "prompt" duty.)
- Will they tell you what was accessed, who was affected, and how they're mitigating?
- Will they cooperate so that you can ethically notify current clients?

Ethics linkage: Rule 1.4 (duty to inform clients of material events), Rule 1.6(c) (reasonable efforts include mitigation), and NYC Bar 2024-3 (prompt investigation, client notice, and improvement).

G. Business Model / Exit Plan

Key questions:

- Can you export all data and files, including but not limited to: audio, documents, video, transcripts, notes, highlights, issue tags, timelines in usable formats?
- If the vendor is acquired (for example, by a law-enforcement-oriented company) can you still access your data under the same conditions outlined by your contract?
- On termination, does the vendor delete your data, certify destruction, and stop using it for 'product improvement'?
- Is the vendor financially stable enough to ensure continued service and security compliance throughout the contract term?

Ethics linkage: Rule 1.1 (competent retention of client material), Rule 1.6 (control and destruction of confidential data), Rule 1.7 (ability to walk away from a conflicted vendor), Rule 5.3 (financial stability as necessary for vendor performance).[17]

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The lawyer should have a remediation plan in place for prompt client notification.") (Diligence: Rule 1.3)

Section 3

Vendor Scorecard

After evaluating a vendor, assign one of three ratings in each domain:

RED ZONE – Unacceptable / Ethical Violation Risk:

- Vendor serves adversarial parties (police/prosecution) in the same jurisdiction or provides technology that creates a structural Rule 1.7 conflict.
- Vendor reuses client data to 'improve products.'
- No guaranteed, rapid breach notice timeline or forensic cooperation.
- No guaranteed right to full data export or destruction.
- Vendor refuses to contractually agree to resist or appeal compelled disclosure.

YELLOW ZONE – Borderline / Needs Mitigation:

- Vendor claims to protect data but allows some ambiguous 'service improvement' use of uploads.
- Vendor uses third-party AI without clearly banning training on privileged defense content.
- Vendor provides security controls but not clear audit log access or subpoena notice.
- You can proceed only if you negotiate protective contract language.

GREEN ZONE – Meets Duties with Documented Safeguards:

- Vendor explicitly bars training AI on your data without written opt-in.
- Vendor contractually segregates defender data from law enforcement.
- Vendor commits to timely breach notice with detail and cooperation (24-48 hours maximum).
- Vendor gives you audit logs, subprocessor transparency, export rights, and certified deletion.
- Vendor commits to resisting compelled disclosure on your behalf.

Suggested Procurement rule:

- A single **RED** in any domain, especially Rule 1.7 Conflict/Alignment, blocks purchase or forces immediate rejection/withdrawal.
- Three or more **YELLOW**s require a written mitigation plan and leadership sign-off.
- **GREEN** across all domains indicates the vendor is structured to satisfy confidentiality, loyalty, supervision, and breach duties.

Section 4

Vendor Due Diligence Questionnaire

Send these questions in writing to every prospective vendor. Keep their answers. This record shows that you exercised 'reasonable efforts' under Rules 1.1, 1.6, and 5.3, and that you evaluated conflicts (Rule 1.7) and communication/breach duties (Rules 1.4, 1.6).

I. Confidentiality and Privilege (Model Rule 1.6)

1. Will you acknowledge in the contract that all uploaded content and its derivatives—including audio, video, transcripts, annotations, stills, timelines, reels, and defense strategy—are confidential and privileged work product? Who owns that content and its derivatives?
2. Do you acknowledge that usage data (including but not limited to usage/access/engagement logs for queries, annotations, transcript, audio, and video) which are defense strategy— is confidential and privileged work product?
3. Can you confirm in writing that our uploads and AI outputs will **not** be used to train or improve any internal or external AI models?
4. Do you or any subprocessor run AI transcription, summarization, tagging, or “insights” on our data? Which models or services perform that work?
5. Do you or your AI providers retain any record of our prompts, uploads, or outputs for product improvement or any other reason?
6. Do you agree that law enforcement or prosecutors or their agents accessing our content and/or usage data absent a subpoena/warrant constitutes a data breach?
7. Can you contractually guarantee that no law enforcement or prosecution agency can access our workspace, usage data, annotations, or analytics derived from our data?
8. Do you carry cyber-liability insurance covering incidents involving our data? Will you attest to that coverage? What is the monetary limit and scope of your cyber-liability and indemnity insurance related to data breaches that could affect privilege or defense clients? Will you show us proof of this coverage?

9. Will your cyber-liability insurance cover law enforcement or prosecutors or their agents accessing our content and/or usage data absent a subpoena/warrant? Will you provide evidence of said coverage?
10. What is your immediate internal protocol when an employee or the company receives a subpoena, warrant, or other legal request ("legal request") for client data?
    a. If you receive a legal request seeking our data, will you agree to:
        i. refuse absent legal compulsion, and
        ii. notify us immediately so we can seek protective relief, unless prohibited by law?
11. What specific contractual and policy measures prevent your employees from discussing, using, or selling information they may learn from supporting the defense organization?

II. Competence and Technology Understanding (Model Rule 1.1; ABA Formal Opinion 512)

1. Do you warn end users that AI output may be incomplete or inaccurate and must be human-verified?
2. Where will our data be stored and processed (physical and regional locations)?
3. List every subprocessor (cloud provider, email delivery, human transcription service, etc.) that can access client data or transcripts.
4. Are all subprocessors bound by written confidentiality, security standards, and rapid-breach-notice duties?
5. Will you notify us before adding or changing subprocessors and allow us to object or terminate?
6. Do you maintain a written incident-response plan, and will you share a summary of it?
7. After detecting unauthorized access or exfiltration of our data, will you notify us without undue delay (e.g., within 72 hours) and include the scope, impact, and mitigation steps?
8. After an incident, will you provide the forensic and audit details we need to meet our ethical duties to notify affected clients?

III. Conflicts of Interest and Vendor Independence (Model Rule 1.7)

1. Do you currently provide products or services to police, sheriffs, prosecutors, investigators, or other law-enforcement entities that involve hosting, analyzing, or indexing digital evidence?
2. If your company serves law enforcement, prosecutors, or courts, what mandatory, internal, and technical firewalls are in place to prevent support staff serving those customers from accessing or seeing any data, activity logs, or metadata related to the defense organization?
3. Do you guarantee that all product improvements derived from Usage Data, Aggregated Data, and Customer Feedback are contractually restricted from being applied, marketed, or developed for the benefit of law enforcement agencies or related prosecutorial entities? How is this monitored and enforced?
4. Do you sell or plan to sell analytics, summaries, or "insights" trained on defender uploads to law-enforcement clients?
5. If our data includes Personal Data subject to the GDPR, will you agree to delete or return all Customer Personal Data within ninety (90) days after the termination of processing, based on our choice?

IV. Personnel Training, Access Controls, and Audit Logging (Model Rule 5.3; ABA Formal Opinions 477R, 498)

1. Do you provide mandatory training for all relevant personnel on the ethical obligations of lawyers, specifically regarding confidentiality, and data handling related to attorney-client privilege?
2. How do you enforce the principle of least privilege? Is staff access to client data (including logs and metadata) restricted based on their role and business need? How do you ensure those restrictions are honored? What is the process for if they are not honored?
3. If any staff (including support or engineering teams) works remotely, what specific security and monitoring protocols are in place to supervise their handling of confidential client data?
4. Do you enforce multifactor authentication (MFA), single sign-on (SSO), and role-based access for all accounts, including vendor-support accounts?
5. Do you maintain immutable audit logs for all access attempts to the defense data, including access by internal technical/support staff? Do these audit logs show which named user (including vendor staff) accessed which file, when, and what they did?
6. Will you provide those audit logs to us on request within 72 hours for litigation, ethics review, or incident response?

V. Third-Party Audits, Data Rights, and Vendor Continuity (Model Rule 5.3; ABA Formal Opinions 477R, 498)

1. Do you agree to submit to standard, jointly approved, independent, third-party security and ethical audits, with results remaining confidential and privileged work product, confirming our supervisory authority?
2. On termination, can we export all original media, transcripts, annotations, highlights, issue tags, and timelines in human-usable formats without punitive fees?
3. Will you agree to delete all original, identifiable Customer Data and other Confidential Information upon the expiration or termination of the agreement, unless that data is retained temporarily in standard backups subject to the Agreement's strict confidentiality restrictions? Will you certify that deletion?
4. Will you agree not to retain any "de-identified," "aggregated," or "product-improvement" copies of our content data after termination unless we explicitly allow it?
5. Do you have anti-retaliation and service-continuity commitments ensuring that our access, pricing, or support will not be affected if we challenge your technology in court?
6. Provide documented proof of your financial health for the past three years, including liquidity ratios, debt-to-equity, and revenue trends, to confirm the PDO can assess vendor-continuity risk.

Section 5

Leadership Due Diligence Checklist

Step 1. Map Your Data

- List every category of data you will upload (body cams, jail calls, police reports, informant audio, strategy notes, client PII, mental health info).
- Mark which are confidential, privileged, or work product.
- This becomes your 'Data Map' and defines what you are ethically obligated to protect under Rule 1.6.

Step 2. Demand Transparency

- Send the expanded Vendor Due Diligence Questionnaire.
- Request supporting materials: security white paper or SOC 2, subprocessor list, incident response policy, breach notice language, sample contract/TOS.
- Request financial reports for the last three years.[17]
- Keep all written answers.

Step 3. Negotiate a Defense Technology Ethics Addendum

- Use the model Addendum in Section 6 below.
- Attach the signed Addendum to the vendor's contract.

Step 4. Score and Document the Decision

- Score the vendor across Domains A–G using the Red / Yellow / Green rubric.
- Note and decide how to proceed if any domain is Red, especially Rule 1.7 Conflict.
  - Suggestion: Do not proceed
- Note and decide how to proceed if three or more domains are Yellow.
  - Suggestion: Create a written mitigation plan and get leadership sign-off.
- Write a short 'Technology Ethics Memo' to your file:
  - What you evaluated
  - Risks you identified
  - Why you concluded the vendor is acceptable ethically
- This memo is your proof of 'reasonable efforts' (Rule 1.6) and competence (Rule 1.1).

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The lawyer should have a remediation plan in place for prompt client notification.") (Diligence: Rule 1.3)

Step 5. Supervise and Re-Evaluate Annually

- Re-run the questionnaire annually or after major vendor changes.
- Ask for updated subprocessor lists and breach summaries.
- Check alignment: did this vendor start marketing to law enforcement in ways that now create a Rule 1.7 conflict?
- Document the review. Ongoing supervision is required by Rule 5.3 and ABA 498.

Step 6. Create Plans to Respond If Something Goes Wrong

Create a document outlining the below steps and ensure multiple people know how to access it and follow it in the event of a breach or problem:

- Contain and mitigate: work with the vendor to stop access or exfiltration.
- Pull audit logs and identify affected clients.
- If a current client's confidential data was materially exposed or your ability to represent them is impacted, notify that client promptly with specifics (Rule 1.4 + Rule 1.6).[5]
- Improve safeguards and, if needed, end the relationship with the vendor.

Step 7. Train Your Team

Train attorneys, investigators, paralegals, and admins on:

- Upload hygiene (what should/shouldn't go in).
- AI output verification (never file raw AI text).
- Breach escalation paths

This meets Rule 1.1 (tech competence) and Rule 5.3 (supervision).

Step 8. Ensure You Are in Compliance With All Relevant Ethical Duties, Noting Key Sources

- ABA Model Rule 1.1 (Competence, including tech competence).
- ABA Model Rule 1.4 (Communication / client notice).
- ABA Model Rule 1.6 (Confidentiality and 'reasonable efforts' to protect data).
- ABA Model Rule 1.7 (Conflicts of interest / loyalty).
- ABA Model Rule 5.3 (Supervision of nonlawyers, which now includes tech vendors and AI tools).
- ABA Formal Op. 477R (secure communication), 498 (virtual practice / supervising vendors), and 512 (generative AI).
- NYC Bar Formal Op. 2024-3 (cybersecurity incident response and client notification).

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512 at 7 (2024). "Lawyers should use professional judgment to determine, based upon the circumstances, whether disclosure of GAI tool use is necessary to comply with Rule 1.4.

Step 9. Procurement Deliverables to Keep On File

- Data Map
- Vendor Questionnaire responses + attachments
- Red / Yellow / Green scorecard
- Signed Defense Technology Ethics Addendum
- Technology Ethics Memo justifying the purchase
- Annual review notes and any breach response records

Section 6

Model Defense Technology Ethics Addendum

Use this Addendum with any vendor that will handle confidential discovery, privileged work product, or client communications. Attach it to the Master Service Agreement, Terms of Service, or equivalent. Some terms are capitalized to reference their contracted definition. If the vendor refuses these terms, that is a warning sign in itself.

1. Purpose

This Addendum is intended to ensure compliance with ABA Model Rules 1.1, 1.4, 1.6, 1.7, and 5.3; ABA Formal Opinions 477R, 498, and 512; and modern cybersecurity guidance. Where this Addendum conflicts with the main agreement, this Addendum controls.

2. Ownership and Confidentiality of Client Data

- All materials uploaded by the Public Defense Office (“Client” or “Client Data”) remain the exclusive property of the Client.
- Vendor will treat all Client Data as confidential and privileged.
- Vendor will not access, disclose, or use Client Data except to provide contracted services, unless required by law and after giving prior written notice to the Client.

3. Prohibition on Data Training and Reuse

- Vendor will not use Client Data, or any derivative of Client Data, to train or improve any machine-learning or AI model (internal or third-party) without express written consent.
- Vendor will not analyze or aggregate Client Data for 'product improvement,' 'quality enhancement,' or marketing, even after the termination of the contract between client and vendor.
- Vendor will not resell, mine, or otherwise repurpose Client Data.

4. Data Segregation and Conflict of Interest

- Vendor warrants that it does not currently provide technology, data analysis, or services to any law-enforcement, prosecutorial, or adversarial customers or where such services would create a Rule 1.7 material limitation conflict.
- Vendor will ensure that no such adversarial customer can access Client Data, usage data, annotations, or analytics.
- If Vendor begins serving law enforcement on shared infrastructure, Vendor must notify Client within 10 days and provide a conflict-mitigation plan; Client may terminate immediately without penalty.

5. Subprocessors and Third Parties

Vendor remains fully responsible for subprocessors:

- Vendor may only use subprocessors listed in an attached Exhibit A.
- Vendor must obtain written approval from Client before adding or changing subprocessors.
- Vendor must bind all subprocessors to confidentiality, security standards, and breach notice obligations at least as strict as this Addendum.
- Vendor must provide documentation showing this to be the case.

6. Security Controls and Audit Logs

- Vendor will implement and maintain safeguards including encryption in transit and at rest, multi-factor authentication for administrative access, vulnerability management, and tamper-resistant audit logging.
- Upon request, Vendor will provide audit logs showing who accessed which Client Data, when, and what actions they took.

7. Breach Notification and Incident Response

- Vendor will notify Client without undue delay and no later than 48 hours after discovering any unauthorized access, disclosure, corruption, loss, or exfiltration of Client Data from their own severs or those of a third party vendor.
- The notice will include: nature of the incident, categories of data affected, scope/impact, mitigation steps taken or planned.
- Compelled Disclosure Defense: If Vendor receives a subpoena, warrant, or court order seeking Client Data, Vendor will immediately notify Client (unless prohibited by law) and contractually commit to assisting Client in mounting every reasonable legal effort to appeal, quash, or delay disclosure prior to compliance. [7]
- Vendor will fully cooperate with Client's forensic investigation and will not notify third parties (including law enforcement) without coordinating with Client unless legally compelled.

[7] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 at 6 (2018). "Best practice dictates that a firm have a breach response plan in place with 'specific plans and procedures for responding to a data breach.'"

8. Data Return and Destruction on Termination

- Upon termination or on request, Vendor will provide all Client Data (including but not limited to media, transcripts, annotations, tags, timelines, and work product) in usable electronic formats within 30 days.
- Within 90 days of termination, Vendor will permanently delete all copies of Client Data (including backups where technically feasible) and certify deletion in writing.
- Vendor will not retain 'de-identified,' 'aggregated,' or 'product improvement' data derived from Client Data.

9. Ongoing Reporting and Audit Rights

- At least annually, Vendor will provide Client with a summary of security audits or certifications relevant to the Services (for example, SOC 2 Type II).[17]
- Client may request reasonable documentation and/or commission independent, third-party security audits to confirm Vendor's compliance with this Addendum.[18]

10. Remedies and Termination for Cause

- Any violation of this Addendum is a material breach.
- Client may immediately suspend or terminate services without penalty if Vendor breaches confidentiality, fails to provide required breach notice, refuses audit, or creates a conflict of interest with law enforcement, as defined by Client.
- Vendor will cooperate in transition, refund prepaid fees for post-termination periods, and assist with secure migration.

Signature blocks should follow, along with Exhibit A (approved subprocessors, their role, and jurisdiction).

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The lawyer should have a remediation plan in place for prompt client notification.") (Diligence: Rule 1.3)

[18] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 11 (2018) ("The duty of competence under Rule 1.1 requires the lawyer to take reasonable efforts to monitor and update security measures... to protect client confidential information.") (Competence: Rule 1.1)

Section 7

Conclusion

Cloud and AI tools are now mandatory to manage modern discovery burdens. The ethical question is not 'can we use them?' The ethical question is 'can we prove that we used them in a way that protected our clients?'

By applying:

- the ethics spine (Rules 1.1, 1.4, 1.6, 1.7, 5.3; ABA 477R, 498, 512; NYC Bar 2024-3),
- the seven risk domains (A–G),
- the Red / Yellow / Green scorecard,
- the expanded Vendor Due Diligence Questionnaire,
- the Procurement & Due Diligence Playbook, and
- the Defense Technology Ethics Addendum.

A criminal defense practice can:

- protect confidentiality,
- maintain loyalty to the client instead of the vendor (by strictly enforcing Rule 1.7 conflicts),
- supervise nonlawyer vendors and AI systems,
- respond ethically to breaches, and
- prove to courts, funders, and bar counsel that it exercised reasonable efforts.

This white paper is intended to be used as part of procurement, onboarding, training, IT policy, and annual vendor review. Vendor will not analyze or aggregate Client Data for 'product improvement,' 'quality enhancement,' or marketing, even after the termination of the contract between client and vendor.

Works cited

Rule 1.1: Competence - American Bar Association, accessed October 30, 2025, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/

Rule 1.1 Competence - Comment - American Bar Association, accessed October 30, 2025, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/

Generative Artificial Intelligence Tools: ABA Formal Opinion 512 Provides Needed Guidance on the Benefits and Burdens of Lawyers' Use of GAI, accessed October 30, 2025, https://thebarexaminer.ncbex.org/article/fall-2024/generative-artificial-intelligence-tools/

Privilege Considerations When Using Generative Artificial ..., accessed October 30, 2025, https://www.frantzward.com/privilege-considerations-when-using-generative-artificial-intelligence-in-legal-practice/

Formal Opinion 2024-3: Ethical Obligations Relating to a ..., accessed October 30, 2025, https://www.nycbar.org/reports/formal-opinion-2024-3-ethical-obligations-relating-to-a-cybersecurity-incident/

ABA Formal Opinion 477R: Securing communication of protected client information, accessed October 30, 2025, https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/

Rule 1.6: Confidentiality of Information - DC Bar, accessed October 30, 2025, https://www.dcbar.org/for-lawyers/legal-ethics/rules-of-professional-conduct/client-lawyer-relationship/confidentiality-of-information

Cybersecurity, Client Confidences, and ABA Formal Opinion 477R, accessed October 30, 2025, https://www.sdcba.org/?pg=FTR-Jun-2017-2

Identifying and Resolving Conflicts of Interest: Three Simple Rules, accessed October 30, 2025, https://www.hinshawlaw.com/en/insights/lawyers-lawyer-newsletter/identifying-and-resolving-conflicts-of-interest-three-simple-rules

ABA Ten Principles of a Public Defense Delivery System - The Gault Center, accessed October 30, 2025, https://www.defendyouthrights.org/wp-content/uploads/ls-sclaid-603-public-def-principles-2023.pdf

Rule 1.7: Conflict of Interest: General Rule - DC Bar, accessed October 30, 2025, https://www.dcbar.org/for-lawyers/legal-ethics/rules-of-professional-conduct/client-lawyer-relationship/conflict-of-interest-general-rule

Rule 1.7 Conflict of Interest: Current Clients - State Bar of California, accessed October 30, 2025, https://www.calbar.ca.gov/Portals/0/documents/rules/Rule_1.7-Exec_Summary-Redline.pdf

Rules of Professional Conduct Rule 1.7: Conflict of interest: Current clients - Mass.gov, accessed October 30, 2025, https://www.mass.gov/supreme-judicial-court-rules/rules-of-professional-conduct-rule-17-conflict-of-interest-current-clients

Rule 1.7 Conflict of Interest: Current Clients - Comment - American Bar Association, accessed October 30, 2025, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_7_conflict_of_interest_current_clients/comment_on_rule_1_7/

5.3 Responsibilities Regarding Nonlawyer Assistants - Board of Overseers of the Bar: Attorney Regulation - Maine Bar Rules, accessed October 30, 2025, https://mebaroverseers.org/regulation/bar_rules.html?id=88243

Rule 5.3 Responsibilities Regarding Nonlawyer Assistance - Comment, accessed October 30, 2025, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/comment_on_rule_5_3/

Vendor Due Diligence Checklist And Questionnaire | Neotas ..., accessed October 30, 2025, https://www.neotas.com/vendor-due-diligence-checklist-and-questionnaire/

Vendor Due Diligence Strategy and Checklist - Mitratech, accessed October 30, 2025, https://mitratech.com/resource-hub/blog/vendor-due-diligence/