[IP Litigator, *Considerations for Responsible Use of AI*, (Jan. 1, 2026)](#)

IP Litigator

[Click to open document in a browser](#)

Considerations for Responsible Use of AI

Matthew Grady and Jonathan B. Roses

Matthew Grady is a shareholder in Wolf Greenfield's Electrical & Computer Technologies Practice who serves as the firm's AI Task Force Lead, helping shape guidance and best practices around emerging AI technologies. He guides clients through the development of effective intellectual property-building strategies incorporating utility patents, design patents, trademarks, copyrights, and trade secrets.

Jonathan B. Roses is a shareholder in Wolf Greenfield's Pharmaceutical Practice. He manages large US and international patent portfolios, advises clients on IP strategy, including regulatory matters related to small molecule and biologic drugs and medical devices, and represents life sciences companies in contested matters, such as post-grant and federal district court proceedings.

I. Introduction

Artificial intelligence, particularly generative AI (GAI), has become an increasingly important component of modern legal practice. Whether you are in-house counsel, outside counsel, or a solo practitioner, the first rule of AI use remains universal: organizations and individuals must ensure the responsible and ethical use of all AI tools. Legal professionals must not only understand the benefits and efficiencies artificial intelligence can provide, but also the obligations, risks, and ethical boundaries that govern its use.

Attorneys operate under some of the most stringent ethical and professional requirements of any industry. As a result, the development of an internal AI use policy must be approached with care, rigor, and an understanding of how AI intersects with legal duties. This article outlines considerations for legal practitioners and their organizations and offers a potential roadmap for any comprehensive AI policy.

II. Attorney Obligations in the Use of Generative AI

A. Competence: Understanding Capabilities, Limitations, and Responsibility

Attorneys must maintain competence in any technology they use, including AI. This duty includes understanding how tools work, what their limits are, and how they handle data. Attorneys must review all AI-generated content for accuracy and rely on independent professional judgment. Regardless of automation, attorneys own the resulting work product and are responsible for errors arising from AI use.

B. Confidentiality and Data Security

Attorneys must assess the confidentiality and security risks of using GAI tools. This includes evaluating data retention, training practices, disclosure risks, and third-party access. Unvetted consumer tools are generally unsafe for legal work.

Special caution applies to trade secrets and personally identifiable information (PII). Even with enterprise systems, uploading trade secrets may challenge the legal requirement to demonstrate reasonable secrecy protections. AI policies should require anonymization, cleaned data sets, and robust data isolation where possible.

C. Supervisory and Management Responsibilities

Attorneys with supervisory authority must ensure policies, controls, and training regarding the use of AI. This includes oversight of staff and vendors, ensuring validation procedures are followed, and monitoring court rules requiring disclosure or certification of AI-related filings.

D. Candor to Tribunals

Attorneys must ensure that no filings, discovery responses, or representations rely on fabricated or erroneous AI-generated content. Duties of candor require verification of all facts, citations, and analyses. Attorneys must also monitor local rules for AI certification requirements.

E. Informed Consent

Clients must provide informed consent before attorneys use AI tools in legal work. This includes disclosure of the tool's purpose, risks, data usage, and alternatives. For in-house counsel, the organization itself is the client and should document approval.

F. Management of Outside Counsel

In-house attorneys should ensure that outside counsel discloses the use of AI, obtains the organization's consent before using GAI tools, and follows the organization's AI policy.

III. Operational and Organizational Considerations

A. AI Usage Logs

For significant matters, organizations should consider maintaining internal AI usage logs documenting tools used, purposes, data involved, validation steps, and security measures. This supports governance and risk mitigation.

B. Periodic Review of AI Policies

AI policies must be periodically reviewed as technology, regulations, and ethical guidance evolve. Updates may be necessary due to court rule changes, bar guidance, vendor policy changes, or new legislation.

C. Cross-Jurisdictional Requirements

Organizations may be subject to the EU AI Act, Canada's AIDA, U.S. state privacy laws, and sector-specific regulations. AI governance must reflect the strictest applicable requirements for compliance.

IV. Special Considerations for Personally Identifiable Information (PII)

PII presents unique risks when processed by AI. Policies should mandate anonymization, data minimization, vendor assurances regarding retention, and restrictions on training models with protected personal data. These steps reduce legal exposure and prevent inadvertent disclosure.

V. Conclusion

AI offers transformative potential for legal practice, but its use must remain grounded in ethical responsibility, professional judgment, and strong governance. By implementing structured controls, validating AI outputs, and maintaining human oversight, attorneys can safely and effectively integrate AI into their practice while upholding their legal and professional obligations.

2   Jan 23, 2026 from VitalLaw®