Patlytics

Exemplary Due Diligence Checklist for AI Tools

For Patent Lawyers and Other IP Professionals at Law Firms and Companies

Patent-Specific Confidentiality

- □ Does the vendor provide sufficient information for compliance with Model Rule 1.6 or similar rules on confidentiality?
- □ Do the vendor's data security practices create any risk of inadvertent disclosure of confidential information?
- □ Are inputs (e.g., IDFs, internal product disclosures) and outputs (e.g., draft patent applications, office action responses, analysis of office actions, FTO analysis) siloed and segregated by customer to prevent co-mingling across the vendor's customers?
- □ Are inputs (e.g., patent numbers) and outputs (e.g., prior art search results, invalidity claim charts, identification of potentially infringing products, infringement claim charts) siloed and segregated by project and client matter?

Attorney Ethics & Professional Responsibility

- □ Does the tool provide citation-backed analysis (e.g., prior art disclosures in an invalidity claim chart) and enable verification of that analysis with the source documents (e.g., prior art reference)?
- □ Does the vendor provide sufficient information regarding the capabilities and limitations of the tool to enable compliance with Model Rule 1.1 or similar rules on competence?
- □ Does use of the tool implicate obligations or rules such as the ABA Model Rules, Formal Opinion 512, state bar opinions, Local Rules of district courts, standing orders of individual judges, and outside counsel guidelines?

AI Output Quality & Reliability

- □ Does the tool incorporate IP expert human review?
- □ Does the vendor disclose accuracy benchmarks?
- □ Does the tool enable user review of outputs?
- □ Does the tool have a citation engine that is able to handle US and OUS patent publications?
- □ Does the tool enable users to verify outputs against source documents?

Patlytics

Exemplary Due Diligence Checklist for AI Tools

For Patent Lawyers and Other IP Professionals at Law Firms and Companies

Data Use & Model Training

- □ Does the vendor train or fine-tune any AI models on customer data (e.g., claim charts, patent applications)?
- □ Does the vendor have any ZDR policies with AI model providers?
- □ Where does data physically reside (e.g., US, EU) and can you restrict residency for matters subject to GDPR or cross-border confidentiality obligations?

Security, Retention & Exit

- □ Does the tool have MFA and how is it enabled?
- □ Does the platform support RBAC with auditable admin access?
- □ What data is retained (e.g., claim charts, patent analysis, patent applications, documents, prompts, embeddings, logs)?
- □ Is tenant isolation documented, with logical segregation from other customers?
- □ Can you verify deletion of all data (including backups) on contract termination?

Incident Response

- □ Is there a clear response procedure or named escalation contacts, not just a generic “security@” or “privacy@” email?
- □ What is the vendor's breach notification timeline, and does it account for the fact that exposure of unpublished applications can permanently compromise patent rights?

This exemplary checklist was developed by Patlytics, the premier AI-native patent platform. Patlytics is purpose-built to meet the criteria on this checklist, including, without limitation, the highest industry standards on security, confidentiality, and data privacy. Learn more at patlytics.ai.