BLACKHILLSAI

WEBINAR · 30 MINUTES · LIVE Q&A

AI Governance for IP Practitioners

Duties, Diligence, and Oversight

Tom Marlow · Chief AI Officer, Black Hills AI



BEFORE WE START

What you'll walk away with

01

Identify where AI use creates professional obligations.

02

Apply seven diligence principles to any AI tool, whether purchased or built in-house.

03

Build oversight that keeps pace with tools that change.

01

Duties

The obligations that attach to you, whatever tools you use.



DUTIES

The duty doesn't delegate

Competence

Rule 1.1, Comment 8: understand the benefits and risks of the technology you use.

Confidentiality

Rule 1.6(c): reasonable efforts to prevent unauthorized disclosure, wherever the information travels.

Supervision

Rules 5.1 and 5.3: responsibility for work done by others, including tools and the vendors behind them.

You can delegate the work. You can't delegate the duty.

DUTIES

Your signature certifies the text



- Your signature certifies the paper: true to your knowledge, reasonable inquiry, warranted arguments
- That holds whether you, an associate, or an AI tool wrote the draft
- The duty of candor stays with you

37 C.F.R. § 11.18 · 37 C.F.R. § 1.56 · USPTO guidance on AI-based tools in practice (2024)

DUTIES

The record is permanent



- Prosecution history is public and read for decades
- It's used in claim construction, estoppel, reexamination, and litigation
- AI-assisted arguments become part of that record when filed
- Watch for over-argument and characterizations of prior art

Prosecution history estoppel · Prosecution disclaimer · Post-grant review

DUTIES

The billing question



- Formal Opinion 512 applies existing fee rules to AI
- Hourly billing covers time actually spent
- Learning a general-purpose tool is overhead
- Flat fees still have to be reasonable

ABA Model Rule 1.5 · ABA Formal Opinion 512 (2024)

02

Diligence



Seven principles behind any AI tool decision, purchased or built.

DILIGENCE · PRINCIPLE 01

Training data

Where confidentiality ends



- Content used for training becomes part of the model
- It can't be recalled or deleted
- The restriction has to cover every provider in the chain

IN PRACTICE

Ask for the contract language, and confirm it flows down to every subprocessor.

DILIGENCE · PRINCIPLE 02

Complexity

A product is rarely one system



- One product can use several models
- Each may come from a different provider, on different terms
- Small AI steps inside a workflow are the easiest to miss

IN PRACTICE

Ask for a feature-by-feature inventory: model, provider, data seen, terms.

DILIGENCE · PRINCIPLE 03

Custody

Knowing where information actually lives



- Something has to store your documents to show them back to you
- Model provider: processes and discards
- Platform: stores what the service needs, under stated controls
- “We retain nothing” is a red flag

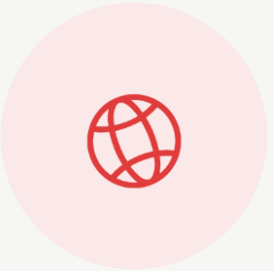
IN PRACTICE

Ask where prompts, outputs, and logs are kept, and for how long.

DILIGENCE · PRINCIPLE 04

Location

Where unpublished work is processed



- Unpublished applications carry confidentiality expectations
- Technical content can raise foreign filing license and export issues
- Processing location matters for patent work

IN PRACTICE

Ask for the specific regions where documents are processed and stored.

DILIGENCE · PRINCIPLE 05

The chain

Privilege doesn't stop at the first vendor

- Confidentiality reaches only as far as the contracts do
- Every subprocessor that touches client content is a link
- One weak contract weakens the whole chain



IN PRACTICE

Ask the provider to name each subprocessor and the obligations that bind it.

DILIGENCE · PRINCIPLE 06

Certification

What a certificate actually covers



- SOC 2 and ISO 27001 cover a scope the vendor defines
- AI features may be newer than that scope
- A certificate covers only what was tested

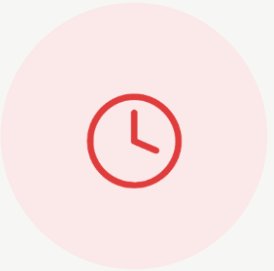
IN PRACTICE

Ask for the scope section and confirm the AI features are in it.

DILIGENCE · PRINCIPLE 07

Change

Why a one-time review goes stale



- Underlying models are upgraded and replaced routinely
- Behavior can change when they are
- A review reflects the tool on the day you did it

IN PRACTICE

Ask what triggers notice of a model change, and what triggers your own re-review.

03

Oversight

Keeping governance current after the tool is in use.



OVERSIGHT

A written AI use policy

Permitted uses

Which tools, for which tasks, with which categories of client information.

Prohibited uses

What never enters an AI tool, and what never leaves the firm without review.

Disclosure

When clients are told about AI use, and how their consent is documented.

The policy is the first thing anyone will ask to see.

OVERSIGHT

Supervision, made operational

Rules 5.1 and 5.3 call for reasonable measures, with named owners.

Who reviews

A named person, assigned before the work starts.

What gets checked

Citations, prior art characterizations, claim language, anything you sign.

How it's recorded

A written record that the review happened.

OVERSIGHT

Review on a schedule

Triggered

A model change, a new subprocessor, or a new AI feature.

Periodic

At least annually, using the same principles.

Owned

A named owner for every AI tool, bought or built.

Applies to tools you buy and tools you build.

OVERSIGHT

When something goes wrong

Plan now for an AI-assisted error reaching a filed document.

Detect

How errors are found and reported internally.

Assess

Candor implications; whether correction or notice is required.

Correct and learn

Fix the record if needed, then update the policy.

RECAP

Duties, diligence, oversight



Duties

They attach to you, whoever or whatever does the work.



Diligence

Seven principles that apply to any AI tool, purchased or built.



Oversight

Named owners, written policy, and review on a schedule.

Questions

Duties, Diligence, and Oversight

Follow-up materials, including Black Hills AI's AI data security disclosure, are available on request.

Tom Marlow · Chief AI Officer, Black Hills AI · blackhills.ai

APPENDIX

What the citations refer to

Model Rule 1.1, Cmt. 8
Technology competence: understand the benefits and risks of relevant technology.

Model Rule 1.6(c)
Reasonable efforts to prevent unauthorized disclosure of client information.

ABA Formal Op. 512 (2024)
Generative AI under the Model Rules: competence, confidentiality, supervision, fees.

37 C.F.R. § 1.56
Duty of candor and good faith in patent prosecution.

35 U.S.C. § 184 · 37 C.F.R. § 5.11
Foreign filing license; also authorizes export of the application's technical data.

Model Rule 1.5
Fees must be reasonable and communicated clearly.

Model Rules 5.1 and 5.3
Supervision of lawyers, nonlawyers, and outside services.

37 C.F.R. § 11.18
Signature certification for papers filed with the USPTO.

35 U.S.C. § 122(a)
Applications held in confidence by the USPTO until publication.

37 C.F.R. Part 11
USPTO Rules of Professional Conduct, which track the Model Rules.