Navigating Regulatory Challenges of AI Tools

Practical Framework for RIAs

BRIGHTSTAR LAW GROUP
RICHARD CHEN

APRIL 2026

What Are AI Tools?

Software leveraging machine learning models

Generate, analyze, or automate outputs

Embedded in business workflows

Includes chatbots and agents

Core Components of AI Systems

Models (LLMs and ML systems)

Orchestration layer

Context layer

Connectors

Models (LLMs)

Trained on large datasets

Generate probabilistic outputs

Examples: GPT-type models

Limitations: hallucinations, bias

Orchestration Layer

Coordinates tasks across tools

Determines workflow execution

Enables chaining of actions

Critical for agents

Context Layer & Windows

Defines runtime knowledge

Includes prompts and documents

Limited by context window size

Impacts output quality

Connectors

Integrate external systems

Enable real-time data access

Expand functionality

Introduce security risks

How AI Tools Work

Prompt + context → processing

Model generates output

Output may trigger actions

Feedback loop refines results

Types of AI Tools

Conversational agents

Notetakers and summarizers

Agentic tools

Workflow automation

Agentic AI Systems

Execute multi-step tasks

Interact with systems

Make rule-based decisions

Higher efficiency, higher risk

Regulatory Lens

Fiduciary duty unchanged

Technology does not reduce obligations

Risk scales with automation

Focus on outcomes

Core Risk Areas

Confidentiality

Accuracy

Bias

Recordkeeping

Regulatory Sources

Investment Advisers Act of 1940

SEC Marketing Rule

Regulation S-P

Books and Records Rule

Enforcement Trends

Misleading disclosures

Weak compliance controls

Vendor oversight failures

Inadequate supervision

Risk Severity

High: Confidentiality

High: Misleading outputs

Medium: Bias

Medium: Recordkeeping gaps

Confidentiality Overview

Client data exposure

Third-party providers

Data retention risks

Cross-border issues

Applicable Rules

Regulation S-P

Safeguards Rule

Duty to protect client info

Vendor oversight

Risk Scenarios

Uploading client documents

Email integrations

Meeting notetakers

Agent system access

Practical Controls

Restrict NPI input

Use enterprise tools

Access controls

Vendor protections

Implementation Guidance

Data classification

Approved tools list

Employee training

Incident response

Accuracy Overview

Outputs may be incorrect

Hallucinations inherent

Overreliance risk

Client impact

Regulatory Framework

Fiduciary duty

Anti-fraud provisions

Marketing Rule

Disclosure obligations

High-Risk Use Cases

Investment recommendations

Performance summaries

Client communications

Compliance documents

Practical Controls

Human review

Source verification

Limit critical use

Review process

Implementation Guidance

Define no-AI zones

Dual review

Audit trails

Staff training

Bias Overview

Embedded in training data

Affects recommendations

Creates unfair outcomes

Hard to detect

Regulatory Implications

Fiduciary duty fairness

Anti-discrimination

Marketing standards

Disclosure expectations

Risk Scenarios

Portfolio recommendations

Client segmentation

Automated decisions

HR tools

Practical Controls

Test outputs

Avoid full automation

Human oversight

Document assumptions

Implementation Guidance

Monitoring procedures

Governance committees

Periodic audits

Vendor diligence

Recordkeeping Overview

Outputs may be records

Dynamic interactions

Audit trail gaps

Regulatory scrutiny

Applicable Rules

Books and Records Rule

Retention requirements

Supervision obligations

Electronic standards

Risk Scenarios

AI-generated emails

Chatbot communications

AI reports

Unlogged agent actions

Practical Controls

Capture outputs

Archive integration

Log prompts

Monitor usage

Implementation Guidance

Define records

Align with archiving

Update manuals

Periodic testing

Case Study 1

AI notetaker deployment

CRM integration

NPI exposure risk

Accuracy risk

Case Study 1 Controls

Vendor diligence

Limit recording

Human review

Archive outputs

Case Study 2

Agentic workflow tool

Multi-system integration

Data accuracy risk

Unlogged actions

Case Study 2 Controls

Limit scope

Require approvals

Log actions

Periodic audits

Final Takeaways

Efficiency vs risk tradeoff

Regulation applies regardless

Governance is critical

Start controlled