

Responsible Use of AI

Data Privacy, Security & Governance Considerations for Certified Financial Planners

Presented at Gulf Coast Estate Planning Conference 2026

Biography of Glenda R. Snodgrass



Glenda R. Snodgrass has been President, lead consultant and project manager at TNE since the company's inception in 1996. She is a Certified Information Security Manager (CISM), CMMC Certified Professional (CCP), CMMC Certified Assessor (CCA), Lead CCA and ITAR Export Control Professional (ECoP®), specializing in helping organizations meet their security and compliance requirements. She has conducted numerous workshops covering GLBA, PCI DSS, HIPAA, FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, NIST CSF and the Cyber Security Model Certification (CMMC). Her dynamic personality and effective teaching style have made her a sought-after public speaker and corporate trainer for more than twenty years.

Fiduciary Duty in the Age of AI

Financial planners must balance
cutting-edge AI capability
with
legal and ethical obligations
to protect client data.



The Fiduciary AI Paradox

Transformative Potential

Generative AI

- automates tedious manual workflows
- parses complex financial documents instantly
- helps draft hyper-personalized financial plans at scale

Ethical & Legal Responsibility

The CFP Board Code of Ethics and Standards mandates reasonable care when adopting technology.

Unregulated AI tools inevitably result in data spillage.

Code of Ethics and Standards of Conduct

CFP Board's *Code of Ethics and Standards of Conduct* reflects the commitment that all CFP® professionals make to high standards of competency and ethics.

14. Duties When Selecting, Using, and Recommending Technology

- a. A CFP® professional must exercise reasonable care and judgment when selecting, using, or recommending any software, digital advice tool, or other technology while providing Professional Services to a Client.
- b. A CFP® professional must have a reasonable level of understanding of the assumptions and outcomes of the technology employed.
- c. A CFP® professional must have a reasonable basis for believing that the technology produces reliable, objective, and appropriate outcomes.

Understanding AI Model Types

Public Consumer Models:

- Ingest user prompts for training.
- Entering client data violates confidentiality rules.

Enterprise SaaS AI:

Operates under Zero Data Retention (ZDR) agreements with isolated tenant architecture to ensure data security.

Private In-House AI:

Self-hosted models provide total control over security boundaries and data lineage.

Security & Compliance Risks

Risk Category	Operational Vulnerability	Regulatory & Ethical Impact
Data Leakage	Client data entered into consumer AI models	CFP Confidentiality & SEC Reg S-P breach
Hallucinations	AI outputs plausible but incorrect	Violation of CFP Board Duty of Care
Shadow AI	Staff using unapproved tools	Supervisory failure under FINRA Rule 3110

Addressing Data Debt

The Barrier to Safe Deployment

Most advisory firms suffer from significant "data debt"—disorganized client records scattered across legacy CRMs, stored files, and emails without standardization.

Turning AI loose on poor data results in inaccurate outputs and unauthorized internal access.

Cleaning data is a prerequisite for AI safety.

Data Governance Principles

1

Identify & Categorize

Inventory all data stores.

Tag or segment Non-Public Personal Information (NPI).

2

Secure

Enforce Role-Based Access Controls (RBAC) so AI models respect strict security boundaries and permissions.

3

Protect

Require signed Zero Data Retention (ZDR) commitments and verify encryption protocols with all third-party vendors.

4

Maintain

Develop and implement written policies and procedures.

Train employees.

Human-In-The-Loop Oversight

Maintaining Fiduciary Oversight

The CFP Board emphasizes that Generative AI should assist human analysis—never replace professional judgment.

Advisors maintain sole accountability for recommendations delivered to clients.

Every AI-generated output must be independently verified by a credentialed planner.

CFP professionals are responsible for the final work product.

AI Deployment Roadmap



Audit Active Tools

Catalog all AI tools across the firm and eliminate unauthorized "Shadow AI."



Secure Vendor Guarantees

Ensure enterprise tools provide tenant isolation and Zero Data Retention (ZDR).



Remediate Data Debt

Clean, structure, and categorize internal file stores before connection to an AI Agent.



Develop a Data Governance Program

Identify & categorize data. Enforce security and protection measures. Develop and implement written policies and procedures. Train employees.



Update Disclosure Forms

Clearly inform clients how AI tools support advisory services.



Implement Review Protocols

Establish mandatory human review procedures for all AI-generated meeting summaries, research memos, and financial plans.

Key Takeaways

Ethical Fiduciary Standard

CFP® Board Guidance for Ethically Integrating Generative AI Into Your Practice

*CFP® professionals should **exercise caution** when using Generative AI for work that requires a reasonable understanding of assumptions and outcomes, such as developing recommendations for Clients...*

*As with any technology, CFP® professionals using Generative AI remain **responsible for their final work product** and must account for Generative AI's limitations and risks.*



<https://theneteffect.com>



[linkedin.com/in/glendasnodgrass](https://www.linkedin.com/in/glendasnodgrass)

grs@theneteffect.com

(251) 433-0196

