TECHNOLOGY

Wealth Think Protecting wealth management data in the age of AI

By Leigh White

Published November 06, 2025, 8:00 a.m. EST | Updated November 06, 2025, 7:59 a.m. EST 3 Min Read

The rise of artificial intelligence has been a swift and disruptive force in wealth management. In just a few short years, the number of large language model-based tools has gone from a handful of early experiments to thousands of platforms flooding the market, with more announced almost daily.

Leigh White, CTO of Myriad Advisor Solutions

For financial advisors, AI's appeal is obvious: faster client communications, automated reporting, streamlined research and the promise of greater efficiency.

But there's a grittier side to this AI revolution that many advisory firms are not yet prepared for.

When employees can freely download, sign up for or experiment with AI tools on company systems, sensitive information is at risk. A seemingly harmless query to "see what this new tool can do" can lead to compliance violations under SEC or FINRA rules, the Health Insurance Portability and Accountability Act, or, for advisors with clients in the European Union, the General Data Protection Regulation. Reputational damage and loss of client trust can follow.

READ MORE: Advisors are using AI but skipping compliance guardrails

The problem is that AI tools behave a lot like young children. Curious learners by nature, they absorb everything around them without fully understanding boundaries. When an employee uploads client data, personally identifiable information or internal financial reports to an AI platform, the tool may log or even store that information so that it's beyond the firm's control.

Even when providers claim not to use customer input for training, risks remain. Data could be cached and exposed if there's a breach. User accounts could be compromised. Misconfigured settings could accidentally make data public.

RELATED

1 What many advisors get wrong about women investors
2 Advisors are in the AI 'apology phase.' Why that won't last
3 AI is taking advisor jobs. It doesn't have to take yours
4 Behind the 'magic' of AI, advisors confront existential risk
5 The antidote to advisors' AI fears: Premium client services

READ MORE: When AI goes wrong in wealth management

That's why wealth firms must harden their networks against such threats by creating the frameworks, policies and technical safeguards to keep client information secure while harnessing the benefits of AI innovatively and responsibly.

"Hardening" isn't a single action; it's a series of practical steps that reduce exposure and enforce guardrails while educating employees about responsible use.

Write down the dos and don'ts

Before rolling out tools, firms must define how AI can and cannot be used. A clearly written policy should spell out protocols and guidelines. Keep it short, clear and actionable. Avoid jargon and write in plain language so every employee understands.

The policy document should include:

- approved tools for business use;
- prohibited activities, such as uploading client personally identifiable information (PII) or financial statements;
- requirements for supervisor approval before experimenting with new platforms; and
- disciplinary consequences for violating policy.

Restrict employee access

Employees should not be able to install or create accounts for AI services without IT approval. Tools to support this policy include:

- application whitelisting/blacklisting;
- identity and access management with conditional rules; and
- network firewalls that block traffic to unapproved sites.

Protect sensitive data

Hardening the network means making it difficult, if not impossible, for sensitive data to "wander" into AI tools. Firms should:

- Implement data loss prevention systems to flag or block risky transfers.
- Enforce encryption on data at rest and in transit.
- Use role-based access controls to ensure only certain employees can view certain files.

Institute regular audits

AI technology evolves fast, and so do threats to its safety. Regular audits of data flow, user activity and system access are essential. Firms should:

- Review logs for attempts to access or upload sensitive information.
- Audit which AI services are being used across the organization.
- Update controls as new risks appear.

Take actionable first steps

If you're wondering where to start, here's a practical roadmap:

- Conduct a risk assessment. Map where PII, client records and proprietary information live. Find where the biggest risks of exposure lie.
- Build in quarterly scheduled reviews and updates. AI is advancing too fast for policies to be static.
- Limit account creation. Use IT controls to ensure only approved services can be accessed from company devices.
- Deploy data loss prevention and monitoring. Even small firms can use affordable cloud-based tools to monitor data flow.

- Train staff on making AI safe as part of your compliance training cycle. This will help highlight risks and reinforce that AI use is not "free play" but a tool to be guided by responsible principles.

Hardening is not about blocking progress, it's about ensuring progress happens safely. By putting the right frameworks in place firms can embrace the promise of AI while protecting what matters most: clients' trust.

Leigh White

CTO

Leigh White, CEPA, is founder and chief technology officer of Myriad Advisor Solutions. She specializes in AI, cybersecurity and technology solutions... Read full bio

TECHNOLOGY ARTIFICIAL INTELLIGENCE CYBER SECURITY REGULATION AND COMPLIANCE WEALTH MANAGEMENT

MORE FROM FINANCIAL PLANNING

What to know about the new IRS digital asset rules

The expansion of cryptocurrency, stablecoins and tokenized assets means more complexity at tax time, including a brand-new form to manage: 1099-DA.

Apr 1, 2026

6 marketing moves to shift RIAs into growth mode

For wealth management firms, organic growth is often tied directly to marketing.

Apr 13, 2026

Help clients through divorce with a nothing-but-net focus

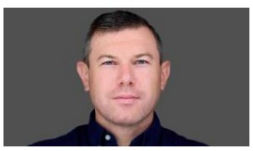
Long-term financial security isn't always served by capturing the biggest account assets. Here's how financial advisors can best serve divorcing clients.

Mar 26, 2026

Private market investments have gone mainstream. Now what?

The intersection between HNW clients and private markets is no longer about distribution, but integration.

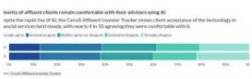
Apr 8, 2026



Older, wealthier clients remain wary of AI. Here's how to build trust

A new report from Cerulli Associates shows older, affluent investors are far more skeptical of AI use than their younger counterparts. Financial advisors who use AI tools in their practices say transparency is key to setting wary clients at ease.

Feb 27, 2026



AI for advisor marketing — without alienating clients

Recent studies have shown that clients and prospects want human authenticity, even as AI tools become more prevalent in firms' workflows.

Mar 31, 2026

CAN RIA GROWTH AND TRUE FIDUCIARY DUTY REALLY COEXIST?

Business goals cannot always put clients' best interests first. Here's why even the executives leading fast-expanding advisory firms say the critics have a point.