RIA Compliance: Moving from "Vendor Trust" to "No Vendor Access"

Author: Matteo Hoch CFP®, EA **Company:** Fin Pods AI Inc **Date:** December 8th, 2025

Executive Summary

As a Registered Investment Advisor (RIA), you operate on a foundation of absolute trust. But a critical, often-overlooked, vulnerability exists in your data workflow: your service providers. When your client uploads a sensitive statement to a standard file-sharing portal, who can *really* see that file?

While these services use bank-grade **AES-256** encryption, they also hold the decryption keys. This means the provider—or a rogue employee, or in response to a subpoena—can access your clients' most sensitive data.

While certifications like SOC 2 verify that a vendor has *policies and procedures* they follow to prevent this, policies are human controls that can fail. We believe a fiduciary standard requires mathematical impossibility, not just policy compliance.

This paper outlines a two-pronged threat:

1. **The *immediate* "Provider Problem":** Your vendors have access to your clients' clear-text data.
2. **The *future* "Quantum Problem":** Malicious actors are stealing this encrypted data *now*, waiting for a quantum computer to break the underlying key exchange—an attack known as "Harvest Now, Decrypt Later."

We present a new fiduciary-grade standard: a **Zero-Access architecture** that solves the Provider Problem, combined with **NSA-grade, hybrid post-quantum encryption** to solve the Quantum Problem. This ensures we cannot leak data we simply do not have the keys to unlock.

---

1. The Immediate Threat: The "Provider Problem"

You rightfully demand that your data is "encrypted at rest" and "encrypted in transit." Nearly every cloud service—including file-sharing portals—claims this using **AES-256** encryption.

This is a dangerous half-truth.

The problem isn't the encryption; it's the *key management*. In a standard cloud model, the *service provider* holds and manages the encryption keys.

This means:

- If a provider employee is malicious or negligent, your client data is exposed.
- If the provider is breached at an administrative level, attackers can access all data.
- If the provider is served with a subpoena, they can be legally compelled to turn over your clients' decrypted files.

The "Compliance Trap": Why SOC 2 Isn't a Silver Bullet You might ask, *"But aren't my current vendors SOC 2 compliant?"*

Fin Pods AI is also SOC 2 compliant. However, it is critical to understand what that actually means. SOC 2 validates **Controls**: it verifies that a company has written policies and procedures to mitigate risk. Essentially, it is a promise that we have put a lock on the door and trained our employees not to open it.

For a fiduciary, a promise is not enough.

- **Standard Compliance (SOC 2):** "We promise not to look at your data."
- **Zero-Access Architecture:** "We *cannot* look at your data, even if we wanted to."

By using **Client-Side Encryption**, we move beyond "Trust but Verify." We never hold the keys, minimizing our risk and yours.

2. The Future Threat: "Harvest Now, Decrypt Later"

While the Provider Problem is an immediate risk, a long-term threat is unfolding: **Q-Day.**

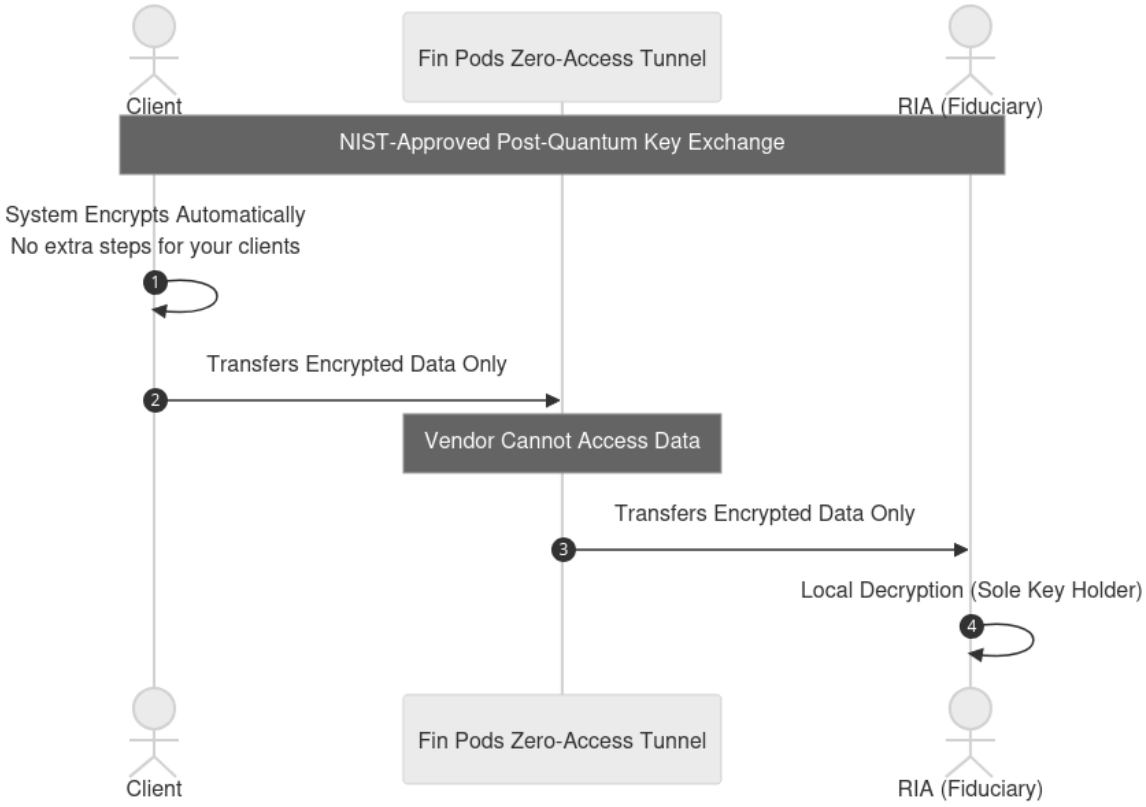
"Q-Day" is the moment quantum computers become powerful enough to break the encryption that underpins the modern internet. Malicious actors are currently executing attacks known as **"Harvest Now, Decrypt Later."** They steal and store encrypted data *today*, waiting for the technology to break the lock *tomorrow*.

The vulnerability lies in the "handshake" used to exchange keys. To protect client data that must remain private for decades (like estate plans), we must upgrade the lock today.

---

3. Our Solution: A Zero-Access, Post-Quantum Vault

Our platform is built to solve both threats simultaneously using a **"No-Knowledge"** approach.



Part 1: Solving the Provider Problem (Zero-Access)

Our guiding principle is simple: **We can't leak data we can't read.** Unlike standard portals, we support a **Zero-Access model**:

- **Direct Encryption:** When your client uploads a document, it is encrypted on *their* device before it ever leaves their computer.
- **You Hold the Keys:** The decryption keys are controlled only by you (the RIA).
- **Encrypted "Blobs":** The file arrives in our system (or your storage) as a meaningless "blob" of scrambled code. At no point does Fin Pods AI possess the ability to view the raw file.

This model protects us, you, and your clients. We already have firms using this today and **it requires no extra steps** from their clients!

Part 2: Solving the Quantum Problem (Hybrid Encryption)

To ensure the "lock" on your data is future-proof, we use an **NSA top clearance-grade** hybrid exchange. We use two locks simultaneously:

1. **X25519:** An industry-leading, high-performance *classical* key exchange algorithm.
2. **ML-KEM-1024:** The new **FIPS-203 standard** for post-quantum key exchange, selected by NIST and recommended by the NSA.

This "hybrid mode" ensures that to break in, an attacker must break *both* the best current technology and the new quantum standard.

---

4. The New Standard: Configurable Security

We recognize that a fiduciary firm has different needs for different types of data. You shouldn't be forced into complex security for a marketing flyer, nor should you rely on standard security for a high-net-worth estate plan.

Fin Pods AI offers a **Configurable Security Model**, allowing you to toggle between Efficiency and Absolute Privacy.

Mode A: Standard Integration (Efficiency)

Best for: Daily operations, low-sensitivity documents.

- **Workflow:** Files are transferred using standard enterprise encryption (TLS 1/AES-256).
- **Benefit:** Maximum compatibility and searchability with Google Drive/SharePoint.
- **Security:** Once transferred to your storage, Fin Pods AI disconnects.

Mode B: The Fiduciary Vault (Zero-Access)

Best for: Estate plans, tax returns, unredacted financial statements.

- **Workflow:** The client's device encrypts the file into a "blob" before upload without any extra clients step. We transfer this encrypted blob to your long term storage provider.
- **Benefit:** Neither Fin Pods AI, nor Google, nor Microsoft can read the file unless you decrypt it. **You hold the only key.**

Bridging the Gap: The "Burn-After-Reading" Engine

A common question is: *"If the file is locked, how can your tool analyze it?"* We solve this with a **Transaction-Based Workflow**:

1. **Targeted Upload:** You authorize the specific document for analysis.
2. **Ephemeral Processing:** We process the file in temporary storage.
3. **Burn After Reading:** The moment the insight is delivered, the raw data is permanently wiped from our system.

This model gives you the best of both worlds: the safety of a cold vault for storage, and the power of advanced analysis—strictly on your terms.

Call to Action

Don't settle for a vendor that dictates your security posture. Choose a platform that protects you through mathematics, not just promises.

To see how our **Zero-Access Architecture** integrates with your existing workflows, schedule a meeting with the Fin Pods AI team today.

References

1. **NIST FIPS 203:** "Module-Lattice-Based Key-Encapsulation Mechanism Standard." *National Institute of Standards and Technology*, August 2024.
2. **NSA CNSA 2.0:** "Commercial National Security Algorithm Suite 2.0." *National Security Agency*, September 2022.
3. **Google Cloud Security:** "Announcing Quantum Safe Key Encapsulation Mechanisms in Cloud KMS." *Google Cloud Blog*, October 2025.
4. **Cloudflare:** "Mitigating the Quantum Threat: Two Migrations." *Cloudflare Blog*, October 2025.