Vendor Due-Diligence Checklist

Version 1.0 · Effective 2026-06-03

PROTOCOL WEALTH, LLC · SEC-REGISTERED INVESTMENT ADVISER · CRD #335298

Use this for every new vendor before any data flows. Start high-level; go deeper only if the vendor touches client information. The goal is a defensible, one-page record that satisfies SEC Regulation S-P service-provider oversight. We record the result in the firm's compliance system and add a row to our Reg S-P service-provider oversight register.

Step 0 The one question that sets the depth

Does this vendor touch client nonpublic personal information (NPI)? — names, SSN/TIN, account numbers, balances, transactions, identity documents.

- **No** (public data only, or firm-operational data only) → light-touch: confirm Steps 1.1–1.3 + reasonable terms, record, done.
- **Yes** → full diligence: all of Step 1 + Step 2.
- **Not sure** → treat as **Yes** until proven otherwise.

Step 1 High-level questions (start here)

1. **What does the vendor do for us, and what data do they see?** (one sentence + the data categories)
2. **Do they publish a SOC 2 Type II (or ISO 27001)?** Where — public, or under NDA via a trust center? *(No verifiable report = a red flag; unverified third-party claims do not count — get the vendor's own report.)*
3. **Do they commit to notifying us of a security breach?** Find the commitment and put it in one of three buckets:

   A — they publish a commitment (a number, or "without undue delay") → cite it.

   B — they publish a security program / SOC 2 but no timeframe → SOC 2 is the anchor; write a one-line reasonableness determination + a PW compensating control.

   C — notification terms are only in our signed contract → pull the clause from the executed agreement.
4. **Where is the data stored?** US-resident? Configurable to US? Or "may be processed in other countries"?
5. **Is there a DPA / data-processing agreement** (public, on request, or in the contract)?

Step 2 Documents to request (vendors that touch client NPI)

- [ ] **SOC 2 Type II** report (current period) — or ISO 27001 certificate
- [ ] **DPA / Data-Processing Addendum** — with an explicit breach/incident-notification clause (target: *without undue delay, no later than 72 hours after discovery*, to PW)
- [ ] **US data-residency** confirmation in writing
- [ ] **Subprocessor list** + commitment to notify on change
- [ ] **Encryption** at rest + in transit (e.g., AES-256 / TLS 1.2+) and access-control attestation
- [ ] Optional: pen-test summary, insurance/cyber coverage, BCP/DR

Step 3 Write the two lines that satisfy Reg S-P

> **Reasonableness determination (one line):** "Commits to notification [the commitment]; assessed reasonable given [SOC 2 / ISO / audit history]; PW compensating controls: [data minimization / US residency / monitoring / zero-data-retention / public-data-only]."

> **Always true:** the obligation to notify affected individuals within **30 days** stays with **Protocol Wealth**, regardless of the vendor. The vendor's job is to tell us in time to start our clock.

Step 4 Decision

- [ ] **Onboard** — diligence complete; bucket A/B with adequate anchor; record in register.
- [ ] **Onboard with conditions** — e.g., pull the breach clause from the contract; obtain SOC 2 under NDA within N days; pin US residency. List conditions + owner + due date.
- [ ] **Do not onboard yet** — missing SOC 2 *and* no breach-notification commitment, or non-US residency with no DPA. Keep client/investor data out until the gaps close.

Step 5 Record

- [ ] Add or refresh the vendor in the firm's compliance system.
- [ ] Add a row to the Reg S-P service-provider oversight register (bucket + commitment + reasonableness determination + compensating control).
- [ ] File any received reports in the firm's vendor-documentation store.
- [ ] If it processes client NPI → it belongs on the public subprocessor list at **protocolwealthllc.com/subprocessors**; the CCO determines materiality and any client notice.

One-page summary (fill one per vendor)

Field	Entry
Vendor / what they do	
Touches client NPI?	Yes / No / Public-only
SOC 2 Type II / ISO 27001	Yes (NDA / public) / No
Breach-notice commitment	(quote) → Bucket A / B / C
Data residency	US / US-configurable / other
DPA available	Public / on request / in contract / none
Reasonableness determination	(one line)
PW compensating control	
Decision	Onboard / Conditions / Do-not-onboard
Conditions + owner + due	
Recorded	☐