agentdatasync Onboarding Runbook

Phased implementation checklist. Nothing moves to the next phase until the current phase's sign-off box is checked. The governing principles throughout: nothing is overwritten silently, agents get read-only access only, and the CCO sees the audit log working before go-live.

Phase 0 — Kickoff & CCO sign-off

Goal: the firm understands exactly what agentdatasync does and does not do, and the CCO approves proceeding *before* any client data moves.

- [ ] Kickoff call held (firm principal, CCO, ops lead, agentdatasync onboarding lead)
- [ ] Scope confirmed in writing: **no money movement, no trading, no advice, no client-facing communication — read-only data access only**
- [ ] Security & Audit whitepaper delivered to CCO; questions answered
- [ ] Service agreement executed, including the **72-hour vendor-to-firm incident notification** clause (Reg S-P service-provider oversight)
- [ ] Sub-processor list reviewed by CCO
- [ ] Due-diligence packet filed in the firm's vendor-oversight records
- [ ] Agents the firm intends to connect identified by name and role (e.g., meeting-prep agent, service agent)
- [ ] Draft permissions matrix circulated (see `templates/agent-permissions-matrix.md`)
- [ ] **CCO sign-off to proceed: _____ Date: _____**

Phase 1 — Data intake

Goal: a complete, untouched copy of the firm's CRM data arrives over a secure channel. The source export is preserved as-received.

- [ ] CRM identified: ☐ Wealthbox ☐ Redtail ☐ Salesforce ☐ Other: _____
- [ ] Export scope agreed (clients, households, contacts, accounts, notes — and what is explicitly *out* of scope)
- [ ] Secure transfer channel established (encrypted transfer; **no client data by ordinary email**)
- [ ] Export received and receipt confirmed to the firm
- [ ] Export integrity verified (record counts reconciled against CRM totals)
- [ ] Original export stored unmodified as the pre-cleanup baseline
- [ ] Any fields the firm flags as sensitive or excluded are documented before cleanup begins
- [ ] **Ops lead confirms intake complete: _____ Date: _____**

Phase 2 — Cleanup

Goal: duplicates resolved, households linked, fields standardized — with the firm approving every material change before it is applied. **Nothing is overwritten silently.**

- [ ] Mapping sheet completed jointly with the firm (`templates/data-cleanup-mapping-sheet.csv`): every source field mapped to a target field with a written transformation rule
- [ ] Duplicate analysis run; candidate duplicate pairs listed for firm review (no auto-merge of client records)
- [ ] Household-linking proposals generated (shared address / shared surname / existing CRM links are *proposals*, not facts)
- [ ] Field standardization rules applied in draft: name casing, phone format, state codes, date formats, account-type vocabulary
- [ ] **Change report produced**: every proposed merge, link, and normalization listed with before/after values
- [ ] Firm reviews change report; merges and links approved, edited, or rejected item by item
- [ ] Approved changes applied to produce the cleaned dataset; rejected items left exactly as exported
- [ ] Post-cleanup reconciliation: record counts and spot-checks against the baseline export
- [ ] Cleaned dataset versioned; baseline export retained for rollback/comparison
- [ ] **CCO or ops lead approves cleaned dataset: _____ Date: _____**

Phase 3 — MCP connection

Goal: the firm's agents can reach the cleaned data — read-only, per-agent credentialed, permissioned per the approved matrix.

- [ ] MCP server installed / configured in the firm's environment
- [ ] Connection verified over TLS
- [ ] **Per-agent credentials issued** — one credential per agent, named for its role; no shared credentials
- [ ] Permissions matrix applied exactly as approved in Phase 0 (deviations require CCO approval)
- [ ] Default field protections confirmed: account numbers **masked**, DOB **year-only** unless the matrix justifies otherwise
- [ ] Tool inventory verified with the firm: exposed tools are **read/search only** — no write, delete, or action tools exist
- [ ] Credential storage confirmed on the firm side (where tokens live, who can access them)
- [ ] Revocation procedure demonstrated: one test credential revoked and reissued
- [ ] **CCO confirms connection configuration: _____ Date: _____**

Phase 4 — First agent query (supervised)

Goal: the CCO watches real queries run and verifies the audit log captures them completely — before any unsupervised use.

- [ ] Supervised session scheduled with CCO (or delegate) present
- [ ] Test queries run per agent role (typical meeting-prep and service lookups)
- [ ] A deliberately **out-of-permission** query attempted — and confirmed **denied and logged**
- [ ] A bad-credential attempt made — confirmed failed and logged
- [ ] Audit log reviewed together: timestamp, agent identity, query, data classes returned, denied/failed events all present
- [ ] Test query run against a masked field — confirmed the agent received the masked value only
- [ ] Log export generated and handed to the CCO in the firm's retention format
- [ ] Agent-output handling agreed: outputs are drafts for human review, never client-ready as-is
- [ ] **CCO approves go-live: _____ Date: _____**

Phase 5 — Go-live & monthly rhythm

Goal: steady-state operation with a compliance rhythm the firm can evidence.

- [ ] Go-live date recorded: _____
- [ ] Firm's staff briefed: what agents may be asked, what they must never be asked to do, how to report a suspected problem
- [ ] Incident contact path confirmed both directions (firm → agentdatasync; agentdatasync → firm's designated contact, incl. after-hours)
- [ ] **Monthly:** CCO completes the audit-log review checklist (`templates/audit-log-review-checklist.md`) and signs off
- [ ] **Monthly:** audit log exported to the firm's records (Rule 204-2 retention: 5 years, first 2 easily accessible)
- [ ] **Monthly:** permissions matrix compared against actual agent usage; unused grants removed
- [ ] **Quarterly:** agent inventory re-confirmed — new agents require Phase 3–4 before use
- [ ] **Annually:** vendor due diligence refreshed (whitepaper, sub-processor list, agreement terms)
- [ ] Offboarding path documented in advance: credential revocation, secure dataset deletion with written confirmation, audit log retained per the firm's instructions