

# VENDOR INFOSEC BRIEF

Commercial Architecture Engagement — Data Handling, Access Control & Regulatory Safeguards

**Prepared by:** Ștefan Prohnițchi    **Audience:** General Counsel / IT Security / Managing Partners    **Classification:** Public Compliance Briefing

**Effective:** September 2026

## 1. SCOPE OF ENGAGEMENT

The engagement focus is restricted to the design and technical implementation of intake workflow automation, Pipeline Triage Gate routing logic, and diagnostic Decision-Support Frameworks. We provide Commercial Architecture; we do not deliver legal, medical, or financial advice. The implementation mechanism operates on a bounded 90-day Deployment Guarantee build phase, transitioning to rolling 30-day maintenance cycles to ensure operational continuity and structural verification.

## 2. DATA DOCTRINE: ZERO-EXTRACTION

To ensure absolute uncertainty resolution regarding data custody, all engagements enforce a strict **Zero-Extraction Protocol**. The core mechanism explicitly prohibits CSV exports of client lists or contact databases. There are no uploads to third-party SaaS platforms outside the practice's approved technological stack. We strictly forbid routing data through external marketing automation tools. All automation and Permanent Infrastructure (CapEx) are built natively inside the practice's existing, encrypted environment, ensuring continuous verifiable compliance.

## 3. ACCESS CONTROL — ROLE-BASED ACCESS CONTROL (RBAC) MATRIX

| PERMISSIONS GRANTED (ARCHITECT ROLE — LEAST PRIVILEGE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | PERMISSIONS DENIED (STRICT BLACKOUT ZONE — ZERO ACCESS)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><b>AUTHORIZED OPERATIONAL ACCESS</b></div> <ul style="list-style-type: none"><li><b>Workflow &amp; Automation Configuration:</b> Native CRM rule gates, stage-transition logic, and intake notification triggers.</li><li><b>Custom Field &amp; Object Creation:</b> Intent-scoring tags, AEV tier parameters, and intake metadata schemas.</li><li><b>Template &amp; Document Assembly Drafting:</b> Pre-consultation educational briefs and structured questionnaire templates.</li><li><b>Analytics &amp; Telemetry Generation:</b> Conversion dwell-time measurement and Money-Denominated Dashboard generation.</li></ul> | <div><b>STRICTLY PROHIBITED ACCESS</b></div> <ul style="list-style-type: none"><li><b>Financial &amp; Billing Access:</b> Zero access to client trust accounts (IOLTA), billing ledgers, or payment merchant logins.</li><li><b>Privileged Document Repositories:</b> Zero access to clinical case histories, legal contracts, or confidential patient charts.</li><li><b>Bulk Data Export Privileges:</b> Database backup extraction and CSV download functions are strictly revoked/disabled.</li><li><b>User Deletion &amp; Governance Rights:</b> Primary administrative domain controls and account provisioning remain client-exclusive.</li></ul> |

## 4. REGULATORY ALIGNMENT

The architectural deployment explicitly conforms to sector-specific compliance frameworks:

- Legal Practices:** Enforces ABA Model Rule 1.6 (Confidentiality) and Rule 5.3 (Nonlawyer Assistance).
- Wealth & Advisory:** Conforms strictly with SEC Regulation S-P and FINRA Books and Records strictures.
- Clinical Practices:** Zero collection of PHI. Operates under standard HIPAA Business Associate Agreements (BAA) and GDPR Art. 28 DPAs.
- Zero Ad Trackers:** No third-party marketing pixels (Meta, LinkedIn) are ever deployed on compliance-sensitive pages or inside secure client portals.

## 5. ARCHITECT VS. EXECUTOR PROTOCOL

The division of labor is a strict security mechanism. We write the CRM queries, structuring the sequencing logic and the underlying architecture for dormant asset reactivation.

However, the internal **Compliance Officer or Managing Partner functions as the final decision function**—reviewing the targeted cohort and triggering final deployment. No external party, including the Commercial Architect, possesses the authority to independently initiate outreach to your client base.

## 6. ASSET SOVEREIGNTY GUARANTEE

100% CLIENT OWNERSHIP FROM DAY 1

Every component of the deployed infrastructure prioritizes your operational autonomy. 100% of the code, CRM workflows, and associated data remain securely on the practice's native stack from Day 1. All administrative credentials remain exclusively with the practice, providing immediate override authority. Upon termination of the engagement, the action protocol dictates a full systemic handoff, resulting in **zero data retention by the vendor**. This represents genuine Asset Sovereignty, eliminating vendor lock-in.