Critique of Gym Agent-in-a-Box Plan

Overall Grade: B+ (7.5/10)

This is a well-thought-out spec with excellent security thinking and real market insight. However, it suffers from scope creep disguised as MVP and several technical gaps.

✅ Major Strengths

1. Security-First Philosophy
   The allowlist approach is exactly right. Most “AI agent” products fail because they give agents too much power. Your constraints are smart:
   - No shell execution
   - No arbitrary code
   - Audit everything
   - Human-in-the-loop gates

   This is actually shippable to risk-averse businesses.
2. Real Problem, Clear Value
   You nailed the gym pain points:
   - Speed-to-lead (within 60 seconds)
   - Show rate improvement
   - Consistent follow-up

   These are measurable, money outcomes. GMs will pay for this.
3. Detailed Data Model
   The SQLite schema is solid - proper relationships, event sourcing via event_queue, good separation between conversation state and message records.
4. Scope Discipline (mostly)
   Clear “must do” vs “must not do” lists. The “no marketplace” stance is commercially smart.

⚠️ Critical Gaps & Issues

1. This Isn’t an MVP - It’s a V1.5
   You claim “MVP” but spec includes:
   - 8 workflows (MVP should be 3-4)
   - 3 script variants (test one well first)
   - Complex state machine with 5+ states

    - Multiple integrations (Twilio + Calendar + LLM)
    - Full audit system

    Real MVP: Lead intake → auto-text → book appointment → send reminder. That's it. Ship in 1 week, not 2.

2. LLM Role is Ambiguous

    You mention OpenRouter/Ollama but never clearly define:

    - Is LLM generating message text? (risky - could say wrong things)
    - Just classifying intent? (safer)
    - Extracting entities? (useful)

    Recommendation: Use LLM only for intent classification and entity extraction. Keep all outbound messages templated. This gives you control + compliance.

3. Desktop App is the Wrong Choice

    Gym managers live on mobile. A desktop-only app means:

    - Harder deployment (download, install, permissions)
    - Can't check leads while walking the floor
    - Limited to whoever is at the computer

    Better: Responsive web app (Next.js/React) with mobile-first UI. Much easier to distribute.

4. State Machine Will Get Messy Fast

    What happens when:

    - User replies after 6-hour TTL expires?
    - Same phone number has multiple leads?
    - User texts during their scheduled appointment?
    - User sends "yes" when you're not expecting booking choice?

    You need explicit timeout handling and context repair logic.

5. Missing Critical Features

Feature	Why Critical
Lead deduplication	Same person fills form twice → duplicate texts
Spanish support	Many gym markets are 50%+ Spanish-speaking
Webhook auth	Anyone could flood `/webhook/lead` with fake leads
SMS rate limits	Carriers have limits beyond Twilio quotas
Image handling	Leads will send photos ("Is this your location?")
Error recovery	What if Twilio is down for 3 hours?

1. Calendar Integration is Harder Than You Think
   Google Calendar OAuth is notoriously painful:
   - Verification process takes weeks for production
   - Refresh token management is fragile
   - Permissions are confusing for non-technical users

   Options:
   - A) Use Calendly/Acuity API (let them handle booking UI)
   - B) Build internal calendar first, add Google later
   - C) Skip calendar entirely for V1 - just send “staff will call to confirm time”
2. Multi-Location Data Model Broken
   You have one settings table but claim to support multiple locations with different scripts/hours/policies. This won’t work.
   Fix: Move script_variant, autopilot_enabled, quiet_hours to locations table.
3. “No Pricing” Policy is a Trap
   Most leads ask: “How much?” Having the agent dodge this kills conversion.
   Better approach:
   - Allow pricing mentions with approval
   - Use ranges: “Plans start at $29/mo”
   - Direct to website: “Full pricing at goldsgym.com/plans”
4. Testing Strategy Absent
   How do you test SMS flows without:
   - Burning Twilio credits?
   - Spamming real phone numbers?
   - Waiting for real-time triggers?

   Need: Mock/demo mode with synthetic leads and simulated time progression.
5. Economic Model Underspecified
   - Who pays SMS overage? (Could be $500+ for high-volume location)
   - OpenRouter costs? (Could be $100-300/mo depending on traffic)
   - Setup fees? (Calendar + Twilio integration is real work)

   Suggest: $299/mo base + $0.03/SMS pass-through + $99 setup fee

🔧 What I’d Change for True MVP
Ship This First (1 week of work):

1. Manual lead entry form (just name + phone)
2. Auto-send ONE templated text:
   "Hi {name}, this is {gym}. Want to tour this week?
   Reply YES for times."

3. If reply contains "yes" →
   Staff gets notification "Lead X is ready to book"
4. Simple dashboard: # leads contacted today

That’s 100 lines of code. You prove the value. Then iterate.
Week 2 Add-Ons:

- Inbound webhook
- Basic intent classification (yes/no/question)
- 2-slot time proposal
- Confirmation text

Week 3-4:

- Calendar integration
- Reminders
- No-show recovery

🎯 Specific Technical Recommendations
Replace This:

Runtime: Desktop app (macOS-first)

With This:

Runtime: Web app (Vercel + Supabase)

- Mobile-responsive
- No installation needed
- Easier updates

Replace This:

LLM: OpenRouter / local Ollama

With This:

LLM: Claude Sonnet via Anthropic API (for intent classification only)

- Reliable

- Affordable ($0.003 per classification)
- JSON mode for structured output

Add This:

```
class SMSRateLimiter:
def can_send(self, lead_id: str) -> bool:
# Max 4 msgs per lead per day
# Max 100 msgs per location per hour
# Max 1 msg per lead per 2 hours
```

Add This:

```
@app.post("/webhook/lead")
async def webhook_lead(
request: Request,
signature: str = Header(...)):
```

```
# Verify HMAC signature
if not verify_webhook(request.body, signature):
    raise HTTPException(401)
```

🚨 Red Flags to Address

1. TCPA Compliance: Need explicit opt-in language + consent tracking
2. A2P 10DLC Registration: Required for business SMS in US (takes 2-4 weeks)
3. SQLite at Scale: Will hit performance limits at ~50k leads per location
4. No Rollback: If bad message goes out, you’re stuck (need unsend/correction flow)
5. Staff Notification: “In-app only” means managers will miss hot leads

📊 Revised MVP Scope

Feature	**V1 MVP (Week 1-2)**	**V1.5 (Month 1)**	**V2 (Month 2-3)**
Lead intake	✅ Manual + webhook	✅	✅
Auto-text	✅ One template	✅ Script variants	✅

Intent classification	✅ Basic (yes/no)	✅ Detailed	✅
Booking	✕ → Notify staff	✅ Propose times	✅ Calendar integration
Reminders	✕	✅ SMS reminders	✅ Email + SMS
No-show recovery	✕	✅	✅
Nurture sequences	✕	✕	✅
Retention saves	✕	✕	✅
Audit log	✅ Basic	✅ Full	✅
Reporting	✅ Simple	✅ Dashboard	✅ Analytics

💰 Business Model Feedback

Your pricing ($199-499/mo) seems too low given the value. Consider:

- Tier 1: $399/mo - 1 location, 500 leads/mo, basic scripts
- Tier 2: $699/mo - 1 location, unlimited leads, custom scripts
- Enterprise: $1,999/mo - 5+ locations, dedicated support

Why this works: If agent improves show rate by just 10%, a gym booking 100 tours/mo gains 10 extra members = $290-490 MRR = $3,480-5,880/year. Your product pays for itself in the first month.

✅ What to Keep (These are Excellent)

1. Allowlist architecture - Perfect for enterprise trust
2. Audit logging - Will save you in disputes
3. Kill switch - Essential for risk management
4. Event queue pattern - Scales well, handles async
5. Opt-out compliance - Non-negotiable legally
6. Human-in-the-loop gates - Smart for high-stakes actions

🎓 Final Verdict

This is in the top 10% of agent specs I've seen because:

- You understand the problem deeply
- Security model is actually thought through
- Data model is solid
- It's buildable

But it's trying to be V2 on day one. Ruthlessly cut to a TRUE MVP:

- One workflow (lead → text → notify staff)

- One script
- Web app, not desktop
- Prove it works in 1 week

Then iterate based on real gym feedback. You’ll learn more from 10 gyms using a simple version than 0 gyms waiting for the perfect version.

Ship fast, get feedback, iterate. That’s how you win this market.