

Below is a **tight 2-week MVP PRD** that bakes in Claude's valid critiques (scope cut, LLM constrained, webhook auth, dedupe, rate limits, compliance) while preserving your core value: **speed-to-lead + bookings**. Claude's main points were: your original "MVP" looked like V1.5 , LLM use must be constrained to classification/extraction only , state machines need timeout + repair logic , and you're missing essentials like lead dedupe, webhook auth, and SMS rate limiting plus TCPA/A2P compliance plumbing .

Gym Agent-in-a-Box MVP PRD (2 weeks)

1) Product definition

Name: Gym Lead Booker (MVP)

One sentence: A locked-down lead follow-up app that **texts new leads within 60 seconds**, offers **two appointment times**, and logs everything for compliance.

Primary outcome metrics

- Median **time-to-first-contact** (goal: < 60 seconds during business hours)
 - **Booked tours per 100 leads**
 - **Reply rate and opt-out rate**
 - **No-show rate** (tracking only in MVP; recovery can be V1.5)
-

2) MVP scope (ruthless cut)

Claude's "true MVP" is basically: lead intake → auto-text → book → reminder . We will ship exactly that, plus the missing safety basics (dedupe/auth/rate limits) and opt-out/compliance tracking .

In-scope (MVP)

1. Lead intake

- Manual lead entry screen

- /webhook/lead endpoint (for your website form) with HMAC auth
- Consent capture fields (checkbox + timestamp + source)

2. Auto-text new leads

- One approved outbound template (no LLM-generated copy)
- Sends within business hours; otherwise schedules next open time

3. Inbound SMS handling

- /webhook/sms inbound endpoint
- Basic intent classification: stop | book | question | other (LLM optional but constrained)
- Two-slot time proposal + “Reply 1 or 2”

4. Booking

- Book into **internal calendar** (SQLite) for MVP
- (Google Calendar integration is deferred to V1.5 per Claude’s timeline suggestion)

5. One reminder

- Single SMS reminder (e.g., 2 hours before appointment)

6. Safety/compliance + ops basics

- Lead deduplication
- SMS rate limits (per lead/day, per location/hour, per lead cooldown)
- Opt-out compliance (STOP handling)
- Basic audit log (who/what/when + payload)
- Global kill switch (disable autopilot immediately)

7. Minimal reporting

- “Leads today” + “Contacted” + “Booked” (Claude notes this can be tiny and still valuable)

8. Staff notification

- In-app notification *plus* optional SMS to manager for “hot lead replied” (Claude warns “in-app only” gets missed)

Out-of-scope (MVP)

- Multiple workflows beyond lead booking (retention, nurture, FAQ engine, etc.)
- Multiple script variants (A/B/C)
- No-show recovery
- Full calendar integration
- Multi-location enterprise controls
- Spanish support (candidate for V1.5 depending on target market)
- Image handling (ignore/deflect politely)

3) Target user and persona

Primary user: Gym GM / Membership Manager who wants more tours booked with less staff inconsistency.

Secondary user: Front desk staff who sees appointments and can manually intervene.

4) User stories (MVP)

1. As a manager, I can connect a work SMS number and set business hours so the system can text leads automatically.
 2. As staff, I can add a lead manually and see the agent text them.
 3. As a lead, I can reply “yes” and receive two time options, then reply “1” to book.
 4. As a manager, I can see today’s leads and how many booked.
 5. As a manager, I can flip a kill switch to stop all automation immediately.
-

5) Functional requirements

5.1 Lead intake

Manual

- Required: name OR “Unknown”, phone (E.164), consent flag, source
- Optional: goal (free text), notes

Webhook: POST /webhook/lead

- Must require **HMAC signature header** (shared secret per location)
- Payload:
 - first_name, last_name, phone_e164, email?, consent=true, consent_text, consent_at, source=“webform”, notes?
- Response: lead_id, dedupe_status

Dedupe rule

- If an active lead exists with same phone_e164 in last 30 days:
- Do NOT auto-text again

- Append note: “Duplicate lead submission”
- Surface in UI as “Duplicate”

5.2 Auto-text behavior

- Target SLA: send within 60 seconds during business hours
- If outside hours: schedule next open time
- If consent is missing/false: do not text; prompt staff to obtain consent (TCPA risk)

5.3 Messaging rules (templated, controlled)

Claude’s recommendation: keep outbound templated, LLM only for intent/entity extraction .

MVP outbound templates

- Initial:
 - “Hi {first_name}, this is {gym_name}. Want to come in for a quick tour? Reply YES and I’ll send two times.”
- Time proposal:
 - “Great. I can do: 1) {slot1} 2) {slot2}. Reply 1 or 2.”
- Confirmation:
 - “Booked: {slot}. Reply RESCHED to change. Reply STOP to opt out.”
- Reminder (2 hours before):
 - “Reminder: your tour is at {slot}. Reply RESCHED if needed.”

Opt-out

- If inbound contains STOP/UNSUBSCRIBE/CANCEL: mark DNC and send one confirmation, then silence .

5.4 Inbound handling + state repair

Claude warns state machines get messy fast and need timeout/repair logic .

States (only 3)

- awaiting_yes
- awaiting_time_choice
- booked

Timeouts

- If lead replies after 24 hours:
- Ignore stale state and restart from safe step:
- “Want to book a quick tour? Reply YES...”

Repair logic

- If expecting “1/2” but receive something else:
- Ask: “Reply 1 or 2, or tell me what time works best (morning/afternoon/evening).”

(You can use a tiny classifier here, but keep outputs JSON and never generate outbound copy.)

5.5 Booking (internal calendar)

- Generate slots based on:
- business hours
- slot duration (30 min)
- buffer (10 min)
- existing internal appointments
- Book into appointments table
- Show “Today” list in UI

5.6 Rate limiting + reliability

Claude explicitly calls for SMS rate limiting and error recovery if Twilio is down .

MVP limits

- Max 4 outbound messages per lead per day
- Max 100 outbound messages per location per hour
- Minimum 2 hours between outbound messages to same lead (unless user just replied)

Retry

- If SMS send fails:
- retry with exponential backoff up to 3 times
- then mark as failed and notify manager in UI

6) Technical requirements

6.1 ActionGateway allowlist

Every side-effect must go through a strict gateway (send_sms, create_appointment, mark_dnc, etc.). This is a core “keep” item .

6.2 Audit log (basic)

Log:

- action_type (SMS_SEND, LEAD_CREATE, APPT_CREATE, DNC_SET, KILL_SWITCH)
- request payload
- provider response or DB result
- success/failure + timestamp

6.3 Data model (minimal tables)

Keep only what MVP uses:

- locations (hours, timezone, gym_name)
- leads (consent fields, status)
- conversations (state)
- messages
- appointments
- event_queue (or a simpler scheduled_jobs table)
- audit_log
- settings (Twilio creds, kill switch)

(Your bigger schema can come later; Claude praised it, but it's not required for MVP shipping .)

7) UX screens (MVP only)

1. Setup

- Gym name, hours, timezone
- Twilio credentials + from number
- Kill switch toggle

2. Leads

- Table: name, phone, status, last message time, booked slot
- Lead detail: transcript + manual “Send” (still via gateway)

3. Appointments

- Today list

4. Reporting

- Leads today / contacted / booked

5. Audit Log

- Filter by lead
-

8) Compliance requirements (MVP posture)

Claude flags TCPA consent tracking and A2P 10DLC registration timelines .

MVP must

- Store consent fields (source, timestamp, consent text version)
- Enforce opt-out immediately
- Provide export of audit log + consent record per lead

MVP should

- Include onboarding warning: “Do not import/text leads without documented consent.”
-

9) Acceptance test checklist (Definition of Done)

1. Create lead manually with consent → initial SMS sends during business hours.
2. Create lead manually outside hours → SMS scheduled for next open.
3. Webhook lead without valid HMAC → rejected (401).
4. Duplicate lead same phone within 30 days → no second SMS; UI flags duplicate.
5. Lead replies “YES” → receives 2 time options.
6. Lead replies “1” → appointment created; confirmation SMS sent.
7. Reminder SMS fires 2 hours before appointment.
8. Lead replies “STOP” at any time → DNC set, one confirmation sent, then silence.
9. Rate limit prevents spamming (simulate 10 sends; verify blocks).
10. Kill switch toggled on → no automated sends occur (scheduled jobs canceled).

11. Twilio failure simulation → retries occur; eventual failure surfaces in UI and audit log.
 12. Export audit log for a lead includes consent + all messages.
-

One-shot Codex prompt (MVP PRD implementation)

If you want to hand this directly to Codex:

```
Build the "Gym Lead Booker" MVP exactly per this PRD:  
- Lead intake (manual + HMAC-auth webhook)  
- Auto-text (1 template) within business hours  
- Inbound SMS handling with 3-state machine + repair logic  
- Internal calendar booking + 1 reminder  
- Dedupe, rate limits, opt-out compliance, audit log, kill switch  
- Minimal UI: Setup, Leads, Appointments, Reporting, Audit Log  
  
Hard constraints:  
- No plugin/skills marketplace  
- No shell execution  
- No LLM-generated outbound copy (LLM optional only for intent extraction JSON)  
- Output only small patches/diffs (no full file rewrites)  
- Include a manual test checklist
```

If you tell me whether you want this as **(A) web app + mobile responsive** (Claude's preference) or **(B) macOS desktop** (your original direction), I'll translate this PRD into a concrete repo plan (tech stack, folder layout, endpoints, and the exact state machine pseudocode) without adding scope.

ActionGateway is a single, centralized layer that all “real-world” side effects must pass through—sending SMS, creating appointments, marking a lead DNC, scheduling reminders, and toggling the kill switch. It enforces a strict allowlist (only approved actions exist), applies safety checks (rate limits, consent required, business hours rules), and writes an audit_log record for every attempt (request + outcome) before returning success/failure to the rest of the system. If an action isn't implemented inside ActionGateway, it cannot be executed anywhere else in the codebase.