FTM SMS Follow-up Automation

Multi-Site Messaging Operations - Comprehensive Technical Overview

A client-readable and engineer-ready reference for automated lead capture, immediate welcome messages, optional business-client booking copies, scheduled follow-ups, marketing broadcasts, inbound reply handling, multi-site routing, verification, operational controls, and current system boundaries.

JotForm | n8n | Google Sheets | Twilio | Webhooks | Scheduled Workflows | Multi-Site Routing

Public technical edition - Evidence reconciled through 20 July 2026

Latest verified changes — 20 October 2026

Read this update first. The July reference that follows is retained in full as historical material. Where older descriptions differ, this dated release note states the current verified behavior and its limits.

BayRidge booking confirmation — LIVE

The existing immediate-submission workflow now keeps and renders the complete BayRidge booking context: service, full name, phone, email, appointment date and time, selected timezone, transactional SMS choice, marketing SMS choice and legal acceptance. The customer and configured business recipient receive the same rendered summary. Registered form routing limits this extension to BayRidge; the other eight active routes retain their existing behavior.

The latest wording adds a friendly greeting, thanks, a welcome, help and a closing. Consent choices display as Yes or No while stored flags remain TRUE or FALSE. Content and label mappings remain configuration data. BayRidge uses 22 saved columns; legacy contacts retain the 19-column contract.

Before and after — current release

Area	Before	After / current status
Booking detail	Welcome text exposed mainly name, date and time.	BayRidge summary includes service, contact details, timezone and consent/legal choices.
Tone and choice labels	Brief confirmation; raw TRUE/FALSE labels.	Warm greeting, thanks, welcome and help; Yes/No display, original stored flags.
Customer and business	Optional copy shared the earlier limited message.	Same complete rendered summary; customer/business delivery verified for earlier wording.
Other websites	Shared workflow with existing route behavior.	Eight other active routes preserved; isolation and live-source parity checked.
BayRidge follow-ups	Disabled; shared monthly defaults named another business.	Twelve correct-brand overrides saved; sending remains disabled pending cost confirmation.
Send-state correctness	Earlier follow-up results could be mismatched or falsely marked sent.	Matched provider acceptance required; failures stay unsent and explicit opt-outs suppress marketing.
Evidence boundary	July reference lacked these later changes.	Current release notes added first; historical material retained; unverified gates stated.

Verification and limits

A controlled public booking test completed successfully before the later instruction against paid tests. Both customer and business-copy messages reached provider status delivered, with three segments each and recorded platform charges totaling $0.04980, plus carrier fees. This proves those two earlier deliveries; it does not prove handset reading or delivery of the subsequently revised warm wording.

The warm revision was checked offline using the re-read live renderer and live template. Customer and business copies matched and retained the complete summary. Routing isolation, missing fields, malformed input, date boundaries and timezone examples passed. All three deployed workflows matched local source. The full template comparison showed only the approved warm-copy and label cells changed.

No paid test texts were sent for the warm wording or follow-up preparation. One test booking from the earlier authorized test remains in the booking system; removal has not been verified.

BayRidge follow-ups — PREPARED, SENDING OFF

Twelve BayRidge-specific messages now cover days 3, 7, 14, 30, 60, 90, 120, 150, 180, 210, 240 and 270 after submission. They use the existing default schedule and follow-up workflow. No additional workflow was needed. Each message uses the correct business identity and contact guidance, includes STOP instructions and avoids invented discounts or clinical promises.

Example, day 3: Hi [name]! Thank you again for choosing BayRidge Beauty. Have a question about your visit or need help? Contact the business using its approved reply details. We're happy to help. Reply STOP to opt out.

The operational templates contain the approved business reply number and website. This public-safe example omits private contact details. Other sites keep their existing templates, schedules and activation flags.

Activation remains FALSE pending the required confirmation of ongoing message charges. At the verified account platform rate of $0.0083 per segment, a two-segment sample costs $0.0166 and the 12-message sample sequence costs $0.1992, plus carrier fees. Actual charges vary with name length, Unicode, carrier, pricing, customer count and opt-outs. These are estimates, not a spending cap.

Activation would include existing explicitly opted-in contacts at future exact-day offsets; it would not replay all missed historical stages. Refresh consent data, due-today preview, pricing and instance timezone before activation.

Follow-up checks and remaining gates

Offline checks executed the actual follow-up selector and renderer for all 12 offsets, explicit refusal, already-sent flags, missed-day non-replay and other-site equivalence. The existing provider-result regression suite passed eight cases. Independent review approved disabled preparation. Sheet read-back proved exactly 48 new values in the intended 12 template rows; Config and formatting were unchanged. No workflow was triggered for testing.

Consent limitation: the current engine skips an explicit FALSE but does not reject blank or unknown marketing consent. The captured BayRidge cohort has explicit TRUE/FALSE values and current intake writes those flags. Do not treat this as a general fail-closed consent guarantee. The cron has three daily checks; its instance timezone needs a fresh check before enabling BayRidge.

Recent platform repairs — dated operational evidence

October 11: follow-up sent-state updates were corrected to require a matched, accepted provider response. Failed or ambiguous sends remain unsent; a confirmed opt-out suppresses marketing. A native credential-free behavioral check verified selective updates and continuation after one site's failures. Public webhook routing and inbound signature checks were also exercised.

October 16: additional platform recovery checks verified public entry behavior and local/live configuration parity in the tested scope. These dated checks do not establish whole-host trust. Detailed incident and recovery evidence remains in the restricted project records.

Release boundary and operator handover

Verified: complete BayRidge summary implementation, earlier two-message delivery, warm-copy offline rendering, other-site isolation, source/live parity and disabled follow-up preparation. Unverified: live delivery of the warm revision, active BayRidge follow-up execution and fresh instance-timezone confirmation. Standalone type, lint, build and CI pipelines are not configured for this data-only follow-up change; security-hook and scoped regression evidence are retained privately.

Operators own approved copy, recipient accuracy, consent and suppression records, quiet-hour policy and review of provider errors. This update does not certify healthcare, privacy or messaging-law compliance. Provider acceptance, provider delivery and customer engagement remain distinct facts.

Historical reference — original July 2026 content

The following sections are preserved verbatim for continuity. Dated claims and recommendations should be read with the current release boundary above.

1. Reading Guide and Publication Boundary

This document serves two audiences. Business stakeholders can focus on the executive overview, operating model, current status, safeguards, and limitations. Engineers can continue through the routing rules, data contracts, workflow responsibilities, failure semantics, deployment controls, and representative traces.

The content is intentionally safe for client and developer review. It explains behavior and engineering decisions without exposing credentials, private resource identifiers, server addresses, internal file paths, private phone numbers, access URLs, authentication flows, or account-specific administration. Authorized operators should obtain those values from the approved secret store and deployment configuration-not from this document.

Truth conventions used throughout:

- Current implementation - behavior supported by the integrated workflow sources and the most recent project verification evidence.
- Historical validation - a dated result retained to explain system evolution; it is not presented as a permanent guarantee.
- Operational control - a required check or practice that protects delivery, routing, or data integrity.
- Known limitation - a verified boundary or remaining improvement stated directly.

2. Executive Overview

Fine Touch Marketing's SMS follow-up platform turns website form submissions into a controlled messaging lifecycle. A customer submits a form, the system resolves the correct client site, records the contact, sends the configured welcome message, and later evaluates that contact for scheduled follow-ups. A separate broadcast lane lets an authorized operator send or schedule approved campaign messages through the same site-aware configuration model.

The platform is designed for many client websites without duplicating the workflow set for each site. Routing, sender selection, message-template selection, reply information, activation state, and follow-up timing are driven by controlled sheet data. The automation code owns the reusable behavior; client-specific wording and routing data remain configuration.

Three workflow responsibilities remain deliberately separate: immediate submission handling, scheduled follow-up evaluation, and broadcast processing. This separation makes failures easier to isolate, allows each lane to be tested independently, and reduces the chance that a marketing operation interferes with form capture.

Current high-level characteristics:

- Central multi-site configuration with site-specific contacts and messaging behavior.
- Immediate contact capture and welcome-message handling after a validated form submission.
- Scheduled follow-ups evaluated against explicit due dates and sent-state markers.
- Instant or scheduled broadcasts scoped to one site or an authorized broader audience.
- Inbound reply guidance assembled from per-site configuration rather than hardcoded client details.
- Operational checks for routing gaps, authentication regressions, missing contact tabs, and deployed-version parity.

3. Product Purpose, Users, and Outcomes

The platform helps Fine Touch Marketing and its clients respond to new leads consistently after web-form submission. Its primary outcome is continuity: every valid lead should enter the correct client data boundary, receive the correct approved message from the correct sender, and progress through the intended follow-up schedule without requiring a separate automation build for every website.

Primary users:

- Prospective customers who submit a form and receive timely, relevant text messages.
- Client operators who manage approved message copy, follow-up schedules, and broadcasts.
- Marketing administrators who onboard sites and verify routing coverage.
- Engineers who maintain shared workflows, deployment integrity, and monitoring.

Explicit non-goals:

- No storage of credentials or secret access material in business-facing documentation.
- No uncontrolled messaging to an unverified form, inactive site, or ambiguous destination.
- No client-specific message text embedded in reusable workflow code.
- No assumption that a provider accepted a message merely because a workflow step started.

4. Current Verified State

The integrated system has active lanes for immediate messages, scheduled follow-ups, broadcasts, and site-aware inbound reply guidance. The latest repair work strengthened routing authority, cross-site isolation, missing-tab handling, delivery-state correctness, and deployment verification. The platform remains operationally dependent on accurate site configuration and on healthy external services.

Verified implementation characteristics:

- A registered form route is authoritative; an untrusted hidden field cannot redirect a submission into another client's messaging path.
- Active sites are evaluated from configuration rather than from a hardcoded list in workflow control code.
- A valid first submission can provision the canonical contact structure without requiring a workflow edit.
- One broken or missing site data area is isolated so it does not abort follow-up processing for every other site.
- Day-one sent state is written only after the messaging provider reports a successful send operation.
- Deployment checks compare editable workflow state with the active published state before completion is claimed.

Historical evidence includes a complete 29-case end-to-end workflow suite from the earlier release cycle, later production incident reproductions, controlled repair tests, and a live missing-site fault-injection check. Those results prove specific behaviors at their recorded dates; ongoing monitoring is still required.

5. System Topology

```
Website form -> verified webhook entry -> route resolution -> site
  configuration -> contact persistence -> welcome SMS
```

```
Scheduled trigger -> active sites -> contact due-date evaluation -> template
  render -> SMS -> sent-state update
```

```
Broadcast trigger -> pending campaigns -> audience selection -> template
  render -> SMS fan-out -> campaign result
```

JotForm acts as the lead-entry surface. A public server-side boundary receives submissions and hands normalized events to n8n. Google Sheets provides controlled configuration, message templates, campaign rows, contact state, and operational records. Twilio provides outbound SMS delivery and inbound-message transport.

The public entry boundary and workflow engine are intentionally separated. The boundary accepts and validates external traffic; the workflow engine performs business routing and state transitions. Internal service locations, authentication material, and provider identifiers are deployment concerns and are intentionally omitted here.

6. Configuration and Data Model

6.1 Config

One row represents one managed site. The row controls the stable site identifier, readable site name, activation state, approved sender reference, template keys, follow-up schedule choices, and optional reply guidance. Deactivating a site should stop new messaging without deleting its historical contact data.

6.1.1 Optional client booking-copy SMS

A business client can optionally receive the exact same rendered day-one message that was accepted for its customer. This feature is controlled entirely from the existing Config row; adding or removing a client does not require a workflow edit or a hardcoded phone number.

To turn the client copy ON for a new or existing client:

• In the Config tab, set reply_phone to the client's verified SMS-capable business number. E.164 format is preferred, for example +15551234567.

• Set booking_copy_enabled to TRUE.

• Set day1_template_key to that client's approved welcome-template key and confirm the key exists in the Templates tab.

Example: site_id = newclient | reply_phone = +15551234567 | day1_template_key = newclient_welcome | booking_copy_enabled = TRUE

To turn the client copy OFF:

Change only booking_copy_enabled to FALSE, or leave it blank. Do not delete reply_phone, because other reply features may use it.

Safety behavior:

• The client copy runs only after the customer's day-one SMS is successfully accepted.

• The copy uses the exact rendered customer message, including approved name, booking date, and booking time variables.

• A disabled flag, blank or invalid client number, empty message, or a client number matching the customer number produces no client-copy send.

• A client-copy provider failure is isolated and cannot undo the saved contact, customer delivery, or day-one sent state.

6.2 Per-site Contacts

Each site owns a separate contact area with a canonical schema. Typical fields include a generated contact identifier, site identifier, customer name, normalized phone number, optional email, submission timestamp, booking context, and sent-state columns for each configured stage. Per-site separation reduces accidental cross-client reads and simplifies client-specific review.

6.3 Templates

Templates are addressed by stable keys. Each row stores approved message copy and an operator-readable description. Workflow code looks up the key at runtime so wording can change without editing or republishing automation logic. Missing keys fail closed for that message rather than silently substituting unrelated copy.

6.4 Broadcast

A broadcast row describes a campaign identifier, audience scope, template key, send-now flag or scheduled date, processing status, timestamps, and result counts. Status transitions must be explicit so a campaign is not repeatedly consumed on every scheduler pass.

6.5 SMS Log and operational records

Delivery attempts and workflow outcomes retain enough context for support without duplicating secrets. Useful fields include interaction lane, site identifier, contact or campaign identifier, event time, provider outcome category, and a safe diagnostic summary. Customer message content and personal data should be minimized according to business need and retention policy.

7. Form Routing and Validation

Correct routing begins before any message is sent. Each production form is registered to one site. When a submission arrives, the platform resolves the form identity against the route registry, confirms that the destination site is active, loads that site's configuration, and only then prepares contact and message operations.

Routing rules:

- Known form plus matching active site -> continue through the site's configured path.
- Known form plus conflicting submitted site hint -> trust the registered route, record a warning, and prevent cross-site redirection.
- Unknown form -> fail safely, record the routing gap, and do not send a client message.
- Inactive site -> retain an auditable outcome without sending.
- Missing required sender or welcome template -> stop the affected send and surface a configuration alert.

The submitted site field remains useful as a diagnostic hint, but it is not treated as authorization. This distinction prevents a copied or manipulated field from selecting another client's sender, contacts, or message content.

8. Immediate Submission Lifecycle

```
Receive -> normalize -> resolve route -> validate configuration -> ensure
  contact structure -> deduplicate -> save contact -> render welcome -> send
  -> mark day-one state
```

The immediate lane extracts supported contact and booking fields from the provider envelope, normalizes the phone value, and resolves the registered site. It then creates or locates the site's canonical contact area and checks whether the same submission has already been processed.

Contact persistence and delivery state are separate facts. The contact may be stored before a send is attempted, but the day-one sent marker is set only after a successful provider response. If delivery fails, the record remains available for controlled retry or support review without falsely claiming that the welcome message was sent.

Duplicate webhook delivery is expected in distributed systems. A stable submission or contact key is therefore used to prevent duplicate contact rows and repeated welcome messages when the source retries the same event.

9. Scheduled Follow-up Engine

The scheduler iterates active sites, reads each site's contacts, computes whether a configured follow-up is due, and checks the corresponding sent-state marker. A message is eligible only when its stage is configured, the due condition is satisfied, the destination is valid, and the stage has not already been completed.

Follow-up safeguards:

- Exact schedule semantics prevent a contact from receiving every overdue stage at once after a prolonged outage.
- Per-stage sent markers make recurring scheduler runs idempotent.
- Site-level failures are contained so healthy sites continue processing.
- The sender and template are loaded from the same resolved site configuration used for the contact.
- Successful delivery is recorded after provider acceptance; failed attempts remain visible for review.

Schedule timing should be interpreted in the approved business timezone. A workflow trigger running hourly does not imply that customers should receive messages at arbitrary overnight hours; operating windows and timezone behavior must remain explicit configuration and verification concerns.

10. Broadcast Processing

Broadcasts use a separate campaign queue so bulk marketing activity does not share the immediate form-submission path. An operator selects a site-scoped audience or an explicitly authorized broader audience, chooses an approved template key, and requests immediate or scheduled processing.

The processor validates campaign status and configuration, selects contacts within the approved scope, renders the template, attempts delivery, records per-recipient outcomes, and updates aggregate campaign state. Partial delivery must remain distinguishable from complete success or complete failure.

Operator controls:

- Use a unique campaign identifier.
- Confirm audience scope before changing status to pending.
- Use approved template keys rather than pasting one-off content into workflow logic.
- Review sent, failed, skipped, and pending counts after processing.
- Respect consent, opt-out, quiet-hour, and applicable messaging rules.

11. Template Rendering and Booking Context

Message templates support reusable placeholders for normalized customer and booking context. The renderer resolves approved fields, handles optional values predictably, and prevents a missing field from producing broken punctuation or raw placeholder text in the final SMS.

```
Hello {first_name}, thanks for contacting {site_name}. We received your
  request for {booking_date} {booking_time}.
```

The example shows the contract, not live client copy. Client-specific wording belongs in the Templates data area. Generic rendering logic belongs in the workflow source and should be covered by tests for present, missing, and malformed values.

12. Inbound Reply Handling

Inbound SMS uses a controlled reply lane that can return site-specific contact guidance. The reply may include an office calling number, an optional text-capable number, and an approved website

reference when those fields are configured. No client number or message is hardcoded in the public request handler.
Cached reply configuration improves response speed, but cache freshness is an operational concern. Updates to reply fields should refresh the cache through the supported workflow, and the response path should fail safely when a site cannot be resolved.

13. Multi-Site Isolation

Every interaction carries one resolved site identity from routing through persistence, rendering, provider selection, logging, and state updates. The same identity must be used at every stage; recomputing it from untrusted fields later in the workflow creates an avoidable cross-client risk.

Isolation invariants:

- A form route resolves to one site.
- A contact is stored in that site's canonical data area.
- Templates and sender configuration come from that same site row.
- Broadcast audience selection cannot escape its authorized scope.
- Warnings and logs identify the resolved site without exposing private access material.

14. Idempotency and Delivery-State Integrity

A workflow run, a provider attempt, and a delivered customer message are not the same event. The system maintains explicit state transitions so retries can distinguish work that never started, work that failed before provider acceptance, work accepted by the provider, and work already marked complete.
The most important invariant is that a sent flag must not move ahead of the real send outcome. Marking a stage complete before the provider call can permanently suppress a message after failure. Conversely, retrying without a stable deduplication key can send twice. The workflow therefore sequences state changes around observable outcomes and preserves identifiers needed for safe reconciliation.

15. Failure Semantics and Graceful Degradation

Expected failure classes and behavior:

- Unknown or ambiguous route -> quarantine the event, alert, and send nothing.
- Inactive or incomplete site configuration -> skip the affected operation and report the missing requirement.
- Missing contact area -> create it when the route is valid and auto-provisioning is allowed; otherwise isolate the site and continue others.
- Template lookup failure -> do not substitute another site's or another stage's message.
- Provider rejection or timeout -> retain unsent state and diagnostic context for controlled follow-up.
- Optional reply-cache failure -> keep the primary submission and scheduled lanes independent.
- One site's processing error -> record it and continue the scheduler for remaining sites.

16. Security and Privacy Boundaries

Credentials belong in the authorized credential manager or environment-specific secret store. Public documentation, workflow descriptions, logs, screenshots, and exported client files must not contain passwords, API secrets, access tokens, authentication cookies, provider account identifiers, private resource IDs, internal host addresses, or server file paths.

Controls expected at the system boundary:

- Treat route hints and form fields as untrusted input; validate types, lengths, and allowed formats.
- Normalize phone numbers before comparison or delivery.
- Restrict configuration editing to authorized operators and preserve change history.
- Apply least privilege to Sheets, workflow, provider, and deployment access.
- Avoid customer message bodies and full personal data in routine logs when metadata is sufficient.
- Protect public webhooks with provider verification, rate controls, and replay-aware processing where supported.
- Maintain consent, opt-out, retention, and deletion procedures appropriate to each client and jurisdiction.

17. Observability and Monitoring

Monitoring should detect failures before a client reports missing messages. Health is measured by business outcomes-valid submissions routed, contacts stored, messages accepted, follow-ups evaluated, campaigns completed-not only by whether the workflow service process is running.

Recommended signals:

- Unknown forms, route mismatches, inactive destinations, and missing configuration.
- Contact persistence failures and missing or malformed site data areas.
- Authentication regressions against Sheets or the messaging provider.
- Provider rejection rate, timeout rate, and messages left pending.
- Scheduler completion by site, including sites skipped after isolated errors.
- Deployment parity between local source, editable workflow state, and active published state.
- Broadcast totals partitioned into sent, failed, skipped, and still pending.

18. Deployment and Version Integrity

The workflow engine distinguishes editable workflow state from the active published version. Updating a draft alone does not prove that production is executing the change. Every deployment must update the intended active representation, restart or reload through the approved mechanism when required, and verify parity after activation.

Deployment gate:

1. Capture and reconcile the current live workflow state before editing.
2. Apply the smallest scoped change to the local source of truth.
3. Run static checks and deterministic regression tests.
4. Publish through the supported deployment procedure.
5. Verify authentication mode, active-site data readiness, and source-to-live parity.
6. Run controlled smoke checks for immediate, scheduled, and broadcast lanes as applicable.
7. Retain a rollback artifact without storing credentials in it.

19. Verification Strategy

19.1 Routing matrix

Cover every active form and include unknown form, inactive site, conflicting site hint, missing route, duplicate delivery, and cross-site isolation cases. A route test passes only when it proves both the expected destination and the absence of unintended destinations.

19.2 Immediate lane

Verify normalization, contact creation, canonical schema, duplicate protection, template selection, provider call, successful sent-state transition, and failure behavior before the sent flag is written.

19.3 Follow-up lane

Use fixed dates to test due and not-due contacts for every configured stage. Include already-sent stages, blank stages, invalid phone data, a missing site contact area, and one failing site among healthy sites.

19.4 Broadcast lane

Test send-now and scheduled campaigns, site-scoped and authorized broader audiences, duplicate campaign runs, missing templates, partial provider failures, and aggregate result counts.

19.5 Deployment verification

Prove that the active runtime contains the tested workflow version and approved authentication configuration. A passing local test is necessary but not sufficient evidence of a correct production deployment.

20. Incident Lessons Incorporated into the Design

20.1 Authentication drift

A workflow edit can unintentionally change a connector's authentication mode even when the business logic appears unchanged. Authentication assertions are therefore part of deployment health, not a one-time setup task.

20.2 One missing site blocked every site

A newly activated site without its required contact structure once caused the scheduler loop to abort. Per-site error containment and first-use provisioning now prevent one configuration gap from starving healthy clients.

20.3 Draft and published versions diverged

A successful edit did not always mean the active runtime had changed. Deployment verification now treats editable state, published state, and running state as separate evidence points.

20.4 Sent state moved before delivery success

Recording completion before provider acceptance could hide failed welcome messages. State updates are now sequenced after the send outcome, and this order is protected by regression tests.

20.5 Routing relied on a submitted hint

A hidden field is convenient context but not a trusted authority. The registered form route now controls the destination, and mismatches are observable rather than silently accepted.

21. Operational Playbook

Before onboarding a site:

- Register each production form to one approved site identifier.
- Create and validate the site configuration row, approved sender, templates, reply fields, and schedule.
- Confirm the canonical contact area exists or that approved auto-provisioning is enabled.
- Submit a controlled test and verify route, saved contact, rendered copy, provider result, and state markers.

Before a broadcast:

- Confirm the audience, consent basis, template, schedule, and quiet-hour rules.
- Use a unique campaign identifier and review a rendered sample.
- Monitor completion and investigate partial results before rerunning.

After any workflow change:

- Run the routing and lane-specific regression suites.
- Verify connector authentication and every active site's data readiness.
- Publish, confirm active-version parity, and run unchanged-lane smoke checks.

22. Known Limitations and Risk Register

- External availability - form, spreadsheet, workflow, network, and messaging-provider outages can delay or prevent processing.
- Configuration quality - incorrect templates, sender references, schedules, or activation state can still produce incorrect business behavior even when code is healthy.
- Delivery semantics - provider acceptance is not the same as handset delivery or customer engagement. Delivery-status callbacks should be used when stronger evidence is required.
- Timezone and quiet hours - business timezone, customer locality, and permissible delivery windows require explicit policy and tests.
- Consent and opt-out - each client remains responsible for lawful consent, content approval, suppression handling, and regulatory compliance.
- Spreadsheet concurrency - human edits and workflow writes can race; stable identifiers and narrow update ranges reduce but do not eliminate this risk.
- Historical totals - dated test counts prove a specific build and environment, not every later configuration change.

23. Recommended Next Engineering Gates

1. Automate the full deployment health check as a mandatory post-publish gate.
2. Add delivery-status reconciliation so provider acceptance and final delivery are reported separately.
3. Add a client-safe dashboard for routing gaps, message outcomes, and campaign progress.
4. Formalize quiet hours, timezone handling, consent evidence, and opt-out suppression per client.
5. Add automated configuration linting for duplicate routes, missing templates, invalid sender references, and unsupported schedule combinations.
6. Define retention and redaction policy for contact data, logs, and exported operational evidence.
7. Run a scheduled test form submission that proves the complete path without messaging a real lead.

24. Technology Stack and Responsibilities

24.1 Entry and orchestration

- JotForm - captures lead and booking fields.
- Server-side webhook boundary - receives external events and forwards validated requests.
- n8n - orchestrates routing, persistence, scheduling, broadcasting, and state transitions.

24.2 Data and messaging

- Google Sheets - stores site configuration, templates, per-site contacts, campaign rows, and operational records.
- Twilio - provides outbound SMS operations and inbound-message transport.

24.3 Verification and operations

- Deterministic regression scripts - validate routing, data contracts, due-date behavior, isolation, and deployment assumptions.

- Health checks and logs - detect errors, configuration gaps, authentication drift, and active-version mismatch.

25. Current Status Summary

The platform is an operational multi-site SMS automation system with separate lanes for immediate welcome messages, scheduled follow-ups, broadcasts, and inbound reply guidance. Configuration drives client-specific behavior, while shared workflow logic enforces routing, state transitions, and isolation.

The most important recent improvements are authoritative form routing, safe unknown-route behavior, per-site failure containment, canonical contact provisioning, post-send state updates, deployment parity checks, and monitoring requirements that focus on business outcomes.

The system should be presented as controlled and production-oriented, not infallible. Ongoing value depends on disciplined site onboarding, approved message content, provider health, consent controls, active monitoring, and verification after every workflow or configuration change.

Appendix A - Representative Request Traces

A.1 Valid first submission

```
registered form -> active site -> canonical contacts area -> new contact ->
  welcome template -> provider acceptance -> day-one sent
```

A.2 Duplicate webhook

```
registered form -> stable submission key already processed -> no duplicate
  contact -> no duplicate welcome message
```

A.3 Conflicting submitted site hint

```
registered form -> route/site mismatch -> registered route remains
  authoritative -> warning recorded -> no cross-site send
```

A.4 One site missing data

```
scheduler -> healthy site processed -> incomplete site isolated and reported
  -> remaining healthy sites continue
```

A.5 Provider send failure

```
eligible message -> provider attempt fails -> sent flag remains false ->
  diagnostic outcome retained -> controlled retry decision
```

A.6 Scheduled broadcast

```
pending campaign -> schedule due -> audience resolved -> template rendered ->
  per-recipient outcomes -> aggregate campaign result
```

Appendix B - Safe Site-Onboarding Checklist

1. Choose a stable, non-sensitive site identifier.
2. Register every production form to that site.
3. Add the site configuration row and leave it inactive during setup.
4. Add approved sender, welcome template, follow-up keys, schedule, and reply guidance. Decide whether the client wants a booking copy; if yes, verify the SMS-capable reply_phone and set booking_copy_enabled = TRUE; otherwise use FALSE or blank.
5. Create or verify the canonical per-site contact structure.
6. Run configuration linting and routing tests.
7. Activate the site and submit a controlled test form.

8. Verify the saved contact, rendered message, provider outcome, and stage state.
9. Record approval and begin monitoring.

Appendix C - Glossary

- Authoritative route - the controlled mapping from a known form to one site; it overrides an untrusted submitted hint.
- Canonical schema - the approved set and order of fields used for each site's contact records.
- Idempotency - the property that safely repeating the same event does not repeat the business effect.
- Sent-state marker - a field recording that one message stage completed after the required send outcome.
- Failure containment - allowing an affected site or operation to fail without stopping unrelated sites.
- Deployment parity - evidence that tested source, editable workflow state, published state, and running state agree.
- Provider acceptance - confirmation that the messaging provider accepted the request; it is not final handset delivery.
- Public technical edition - documentation designed for broad professional review without private access material.

Appendix D - Review Checklist

For client review:

- Confirm approved wording, timing, audience rules, reply guidance, consent, and opt-out process.
- Confirm every active website and form has an accountable owner.
- Confirm the reported limitations and provider-delivery semantics are understood.

For engineering review:

- Trace a submission through route authority, contact persistence, template selection, provider outcome, and state update.
- Verify a bad site cannot block healthy sites or access another site's data.
- Verify tests cover unknown, duplicate, inactive, mismatch, missing-data, authentication, and publish-parity cases.

For operational review:

- Confirm monitors detect business failures, not only process uptime.
- Confirm rollback artifacts and current deployment evidence are available to authorized maintainers.
- Confirm exported client material contains no credentials, secrets, private IDs, internal paths, or private contact details.

Developed by Zahidul Islam

Workflow and backend engineering - multi-site routing, delivery-state integrity, operational reliability, and client-safe automation.