CAPMINDS

ENTERPRISE IMPLEMENTATION PLAYBOOK

24/7 Managed Integration NOC Playbook + 5-Year Cost Model

A decision and implementation guide for U.S. health systems

A green interface dashboard can hide a clinical outage.

An integration engine can accept a message, empty its queue, and still leave a clinician without a usable result. The operational contract must therefore extend from transport availability to verified delivery at the agreed application boundary. Otherwise, a supplier can meet its infrastructure SLA while the hospital absorbs the clinical consequences.

This playbook defines a managed integration Network Operations Center (NOC): continuous detection, triage, controlled recovery, and evidence of restoration across HL7 v2, FHIR APIs, and batch interfaces. It separates those responsibilities from clinical decisions, application ownership, and security incident command.

The leadership decision

Buy an accountable operating capability, not an unspecified pool of monitoring hours. Approve a service boundary, named escalation owners, replay authority, tested recovery objectives, and a cost model before agreeing to a monthly fee.

Read for	Pages
Operating scope and clinical priorities	2-3
Monitoring, incident response, and replay	4-5
Resilience and implementation gates	6-7
Five-year economics and procurement	8-9
Operational templates and source register	10-11

Define the boundary before you promise coverage

The highest-risk gap is usually between owners. A hospital owns the EHR, a laboratory owns the sender, a network team owns the VPN, and the integration supplier owns the engine. A managed NOC must coordinate this chain even where it cannot change a component.

Create one operational record per production flow

Record interface ID; sending and receiving organizations; clinical purpose; message/resource types; transport; engine channel and version; endpoints; authentication owner; certificate expiry; expected schedule; peak volume; dependency map; recovery tier; and named business and technical owners. Include the acknowledgment boundary: engine acceptance, destination application acceptance, or downstream reconciliation.

Accountable party	Required responsibility
Hospital service owner	Approves clinical priorities, downtime activation, data correction, and restoration acceptance. Maintains an executive escalation path.
Managed NOC	Detects and triages; preserves evidence; executes approved runbooks; coordinates vendors; maintains incident timeline and shift handoff.
Integration L2/L3	Diagnoses mapping, routing, queue, and runtime faults; authorizes technical recovery within change controls.
EHR / source owner	Confirms application ingestion and business-state correctness; resolves source identifiers and application rejects.
Security operations	Owns suspected compromise, evidence preservation, containment decisions, and breach assessment. NOC remains operational coordinator.

Write exclusions as handoffs, not dead ends

If a vendor API is unavailable, the NOC may not repair it, but must open the vendor case, track retries and backlog, notify the clinical owner, and reconcile delivery after recovery. Define who pays for new interfaces, historical cleanup, mapping changes, and extended vendor incidents.

Acceptance evidence: every critical flow has a primary and backup owner; the contact tree is exercised outside business hours; access works from the support environment; and each excluded action has an accepting team. An unanswered escalation is a service defect.

Translate patient impact into measurable commitments

Do not assign severity solely from server health. One delayed critical-result feed may matter more than a million delayed analytics records. Agree clinical tolerances with the affected service; a NOC cannot invent them after an incident begins. SAFER guidance supports this clinical and technical coordination.

Illustrative priority	Trigger and initial response target
P1: immediate coordination	Potential patient-safety impact, widespread critical delivery loss, or suspected corruption. Human acknowledgment within 5 minutes; incident bridge within 15; updates every 30 minutes.
P2: material degradation	Growing backlog or partial failure with an available workaround. Acknowledge within 15 minutes; updates hourly until stable.
P3: bounded exception	Nonurgent single-flow failure within an approved delay tolerance. Acknowledge within 60 minutes during contracted coverage; assign a resolution plan.

Use three clocks

- **Detection:** first measurable breach to alert.
- **Response:** alert receipt to a named human taking ownership.
- **Recovery:** service impact begins to verified restoration. Keep vendor waiting time visible in gross elapsed time even if a contract excludes it from a particular SLA calculation.

Measure what the receiving workflow needs

Track eligible transactions delivered within their clinical time budget divided by eligible transactions expected. Define treatment of duplicates, canceled orders, invalid source records, maintenance, and missing source events. Reconcile against the sender or schedule; engine-only counts cannot detect messages that never arrived.

A proposed 99.9% monthly time-availability target allows 43.2 minutes in a 30-day month. It says nothing about message correctness or latency. Report availability, freshness, oldest queued age, reject rate, and reconciliation exceptions separately. Use SLO burn-rate alerts where volumes support meaningful ratios; use deadline-based controls for sparse events.

Restoration is a signed event

Record four milestones separately: live-service restoration, backlog clearance, reconciliation completion, and incident closure. Define the contractual recovery endpoint in advance. Quarantine alone does not resolve clinical impact: the hospital owner must accept remaining exceptions, with a workaround, owner and deadline. Delivery acceptance does not establish clinician review or follow-up.

Build detection around failure modes

A heartbeat proves that a process is alive. It does not prove that ADT demographics reach the right chart, that a result is filed, or that a scheduled batch contains the expected records. Combine transport telemetry with workflow-specific controls.

Failure mode	Detection and first investigation
Silent source / missing batch	Use deadline-based missing-event alerts for sparse flows. For files, check manifest, control totals, checksum and completion marker; reject partial or duplicate files and preserve restart checkpoints.
Queue growth	Track oldest age, enqueue/dequeue rate, retry count, and disk runway. Compare arrival rate with sustainable drain rate.
HL7 reject / uncertain ACK	Correlate MSH-10 with MSA-2. In enhanced mode, CA means commit acceptance; AA reports application acceptance. Inspect CE/CR, AE/AR and ERR. Record MSH-15/16 behavior; neither stage proves clinician review.
FHIR / authentication fault	Inspect each batch Bundle.entry.response.status: outer HTTP 200 can contain failures. Distinguish batch from atomic transaction. Check authentication, throttling and OperationOutcome where returned.
Semantic misdelivery	Reconcile identifiers, encounter links, code mappings, and destination application state. Escalate mismatches to application ownership.
Capacity / certificate risk	Alert before storage exhaustion and certificate expiry; assign renewal owners and test dependencies after rotation.

A practical event envelope

Attach interface ID, environment, direction, source event time, engine receipt time, destination acknowledgment time, correlation ID, attempt number, configuration version, and incident link. Preserve timezone and clock-synchronization status. Hash or tokenize identifiers where feasible; correlation metadata may still be sensitive.

Separate operator visibility from payload access

Send operational metadata to paging and ticketing systems. Keep patient payloads in access-controlled systems with approved retention and audit logging. Do not paste clinical messages into general chat. HHS cloud guidance makes BAA and responsibility allocation material to the design.

Alert quality gate: each paging rule names an owner, impact statement, runbook, and recovery signal. Group downstream symptoms under the incident without suppressing unrelated critical flows. Review false pages and missed detections weekly.

Recover without creating a second incident

Illustrative scenario: the receiving EHR resumes after a 40-minute interruption. The queue begins draining, but retries duplicate orders that were committed before connections timed out. The outage has ended; the data-integrity incident has just begun.

Runbook: destination outage with uncertain delivery

1. Establish scope. Identify affected flows, last verified delivery, oldest outstanding item, and clinical impact. Preserve logs and configuration versions. Activate the agreed clinical downtime process through the hospital owner.

2. Stabilize. Cap retry concurrency and apply bounded backoff. Quarantine defective messages together with dependent work where required. A failed patient or encounter event may require holding its downstream orders; continue only unrelated transactions whose processing is safe. Avoid purging queues or resetting offsets to make the dashboard green.

3. Determine commit state. A missing ACK or HTTP timeout is not proof of failure. Reconcile sender ID, engine state, and destination evidence. Where commit state cannot be established, hold uncertain items for application-owner review.

4. Authorize a bounded replay. Record the message range, sender namespace, business identifier, correction/version semantics, deduplication window, exclusion list, destination, configuration version, approver, maximum rate, and stop conditions. Validate deduplication semantics for that destination; do not assume every API operation is idempotent.

5. Drain and reconcile. Start with a small approved sample. Check application results before expanding. Preserve clinically relevant ordering, such as patient/encounter context before dependent orders, according to the interface specification.

Backlog recovery is a capacity calculation

If backlog B = 120,000 messages, new arrival rate = 80 messages/second, and validated destination capacity = 180/second, theoretical drain time is B / (180 - 80) = 1,200 seconds, or 20 minutes. If capacity falls to 80/second, the backlog cannot drain. This estimate excludes rejects, dependencies, throttling, and revalidation.

Stop conditions and closure evidence

Stop replay on new duplicates, rising reject rates, breached clinical ordering, or destination degradation. Archive pre/post counts, replay manifest, quarantine reasons, application validation, and approver. Correcting a downstream clinical record may require a compensating workflow; rolling back engine code will not undo that record.

Engineer recoverability and controlled access

High availability protects against selected component failures. Disaster recovery addresses loss of a larger failure domain. Neither guarantees that transactions were applied once, in order, or to the intended patient. Test the data path as well as the platform.

Make RTO and RPO concrete

Define recovery time objective (RTO) as the allowed restoration interval and recovery point objective (RPO) as tolerable data loss, separately for each flow tier. An illustrative critical-flow target is RTO 30 minutes and RPO 5 minutes; clinical owners must approve or replace it.

Measure engine-state RPO separately from recoverable source transactions. Verify sender replay retention covers the recovery gap. Include queue persistence, configuration, secrets and routing; a recent database backup alone does not establish end-to-end data recoverability.

Control	Implementation evidence
Failover and fencing	Prove that each work item has one authorized processing owner; supported partitioned or clustered consumers may run concurrently. Test lost connectivity and split-brain prevention, not only planned shutdown.
Backups and restore	Restore engine database, configuration, and required keys into an isolated environment. Verify queue and message-state consistency.
Access and secrets	Named accounts, MFA-protected administrative access, least privilege and audited emergency access. For legacy endpoints, document approved gateway controls, residual risk and a remediation owner.
Change management	Version mappings and routes; test representative synthetic cases; approve rollback conditions; reconcile transactions spanning a deployment.
Security coordination	Route suspected compromise to security command. Preserve relevant evidence before destructive recovery actions.

A resilience exercise must generate a recovery record

Record failure injection time, detection time, human ownership, failover execution, first successful business transaction, backlog completion, and reconciliation outcome. Compare actual RTO/RPO with targets and assign gaps. Run after material topology changes and at a risk-approved recurring interval; quarterly critical-flow exercises are a planning proposal, not a universal mandate.

Retention periods must follow applicable obligations, contracts, and risk assessment. HIPAA documentation retention requirements should not be presented as a blanket mandate to retain every interface payload or log for six years. Confirm payload and audit-log schedules with privacy and records-management owners.

A 90-day transition with explicit go/no-go gates

The calendar is illustrative. A hospital with unidentified interfaces or unreliable destination evidence should extend discovery rather than transfer operational risk through a ceremonial go-live.

Stage	Deliverable and exit gate
Days 1-15: baseline	Inventory critical flows and dependencies; measure volume, queue age, exceptions, page load, and current costs. Exit: clinical owners approve tiers and missing evidence is assigned.
Days 16-30: instrument	Configure telemetry, correlation, access, escalation, and first runbooks. Exit: injected failures generate the correct alert and reach an available owner.
Days 31-60: shadow	NOC shadows incumbent operations; tests handoffs, uncertain delivery, replay, and restore. Exit: operators demonstrate recovery without undocumented expert intervention.
Days 61-75: controlled transfer	Transfer a bounded flow set with rollback coverage. Exit: stable paging, reconciled transactions, and accepted daily exception reports.
Days 76-90: acceptance	Run an off-hours P1 exercise and a recovery test. Exit: hospital owner signs coverage, recovery evidence, unresolved-risk register, and monthly scorecard.

Staff the workload, then staff the clock

One continuously occupied seat requires 8,760 coverage hours per ordinary year. At 2,080 paid hours per FTE and assumed 25% unavailability for leave, training, and other noncoverage time, productive coverage is 1,560 hours: 8,760 / 1,560 = 5.62 FTE. Round to six for planning. This does not provide a second simultaneous seat, specialist depth, or guaranteed surge capacity.

The model on page 8 adds two integration specialists and a separate specialist-support allowance. Two specialists alone do not establish sustainable round-the-clock L2/L3 coverage. Validate primary/backup rotation, callout pay, leave, vacancy cover, engineering time and simultaneous incidents. A shared managed service may pool coverage across clients; require evidence of concurrent-incident capacity, named L2/L3 response, shift handoff, and substitute staffing. Do not equate a vendor hotline with a dedicated 24/7 operator.

Monthly service review

Review clinical delivery SLOs, incidents by flow, oldest unresolved exceptions, replay volumes, repeat failures, after-hours pages, recovery-test results, and cost per managed production flow. Assign an owner and deadline for the top recurring fault; monitor whether the fix actually reduces operational demand.

Cost inputs: compare three operating models

Launch scope: 100 governed production flows, growing 10% annually.

- A is a new dedicated internal monitoring seat;
- B is shared managed coverage;
- C retains internal integration engineering and buys shared monitoring/triage.
- B and C require contractual proof of capacity, escalation and concurrent-incident handling before they can be treated as service-equivalent.

Year-1 annual input	A: Internal	B: Managed	C: Hybrid
Coverage: 6 x $100k x 1.30	$780,000	In fee	In fee
Specialists: 2 x $140k x 1.30	$364,000	In fee	$364,000
Hospital owner: 0.5 x $150k x 1.30	$97,500	$97,500	$97,500
Specialist backup / callout allowance	$60,000	In fee	$60,000
Unquoted service fee	$0	$420,000	$180,000
Engine / support allowance	$60,000	$60,000	$60,000
Infrastructure allowance	$72,000	$72,000	$72,000
Monitoring / ticketing allowance	$24,000	$24,000	$24,000
Exercises / training	$20,000	$20,000	$20,000
Year-1 recurring	$1,477,500	$693,500	$877,500
Year-0 transition	$150,000	$100,000	$80,000

Service inputs are $35,000/month for B and $15,000/month for C, selected solely to demonstrate the model. C buys continuous shared monitoring/triage; the hospital retains engineering and specialist escalation. The $60,000 backup allowance in A/C must be replaced with a roster or support contract that actually meets the required response.

Annual salaries already include paid leave. The assumed 30% salary loading covers additional employer costs; shrinkage reduces available coverage hours, not salary. Do not equate 30% of salary with benefits at 30% of total compensation or add paid leave twice. BLS sources are benchmarks, not integration-specific wage evidence.

Transition allocations (A/B/C, $000): discovery 30/20/15; access and telemetry 35/25/20; runbooks and training 35/20/15; shadow support and acceptance 50/35/30. Replace each with priced work and accountable ownership.

Five-year cash flows and decision sensitivities

Escalate labor, support allowances, fees, training and license renewals by 3% annually. Infrastructure grows 8%; tooling grows 5%. These are independent planning assumptions, not vendor forecasts.

No license capacity step is included: Mirth prices per production server, so validate server/tier and HA/DR entitlements separately.

USD, rounded	A: Internal	B: Managed	C: Hybrid
Year 1	$1,477,500	$693,500	$877,500
Year 2	$1,525,905	$718,385	$907,905
Year 3	$1,576,074	$744,329	$939,534
Year 4	$1,628,085	$771,387	$972,448
Year 5	$1,682,018	$799,619	$1,006,712
Year 0	$150,000	$100,000	$80,000
5-year nominal total	$8,039,582	$3,827,219	$4,784,100

Formula for year t: base x 1.03^(t-1) + $72,000 x 1.08^(t-1) + $24,000 x 1.05^(t-1). Base includes the $60,000 license allowance. Add transition once. Totals use unrounded values; rounded rows may differ by $1. No savings percentage is claimed: service equivalence remains a procurement gate.

Test the assumptions that drive the ranking

If B fees rise with 10% annual flow growth as well as 3% escalation, add $508,129; B becomes $4,335,348. Every extra $10,000/month of initial fee adds $637,096 over five years. A second dedicated coverage seat adds $4,141,126, before equipment or specialist capacity.

Show full economic cost and incremental cash expenditure separately. If existing staff are reassigned, their allocated cost does not become cash savings. Count only demonstrably avoided hires, overtime, contracts and infrastructure as avoidable expenditure. C is a full-cost scenario; existing capacity must be separately credited in an incremental budget.

Excluded: taxes, financing, major EHR replacement, unplanned projects, downtime losses and exit fees. Price exit assistance separately. For NPV, discount year-end nominal cash flows at a hospital-approved nominal rate; year-0 transition is not discounted. Validate flow-growth capacity rather than assuming unchanged staffing is adequate.

Four operational records to put into use

Copy these field sets into the service-management system. Record evidence links and approver identity; an unchecked field is an unresolved acceptance item, not an implicit approval.

Record	Required fields and completion rule
Interface acceptance	Flow ID / version; clinical owner; technical primary and backup; source/destination; protocol; ACK boundary; freshness deadline; expected volume; dependencies; reconciliation method; replay retention; recovery tier; test evidence; approver/date. Approve only after normal, failure and recovery paths pass.
Replay authorization	Incident ID; sender namespace; business key and version; start/end range; uncertain commits; held dependencies; dedupe window; configuration version; destination; approver; sample size; rate cap; stop conditions; before/after reconciliation. Stop if scope or semantics change.
Shift handoff	Outgoing/incoming operator and time; active incident severity; oldest unresolved item; patient-impact owner; pending vendor actions; temporary changes and expiry; next action/deadline; escalation contacts. Incoming operator explicitly accepts handoff.
Supplier comparison	Shared/dedicated staffing; coverage hours; primary/backup L2/L3; concurrent-incident capacity; response/update targets; workload bands; included engineering; exclusions; BAA/subcontractors; license/environment rights; transition/renewal/exit charges; evidence and deviations. Compare only accepted service scopes.

Minimum acceptance test pack

Test a lost ACK after destination commit; an HTTP-200 batch with a failed entry; a missing or partial file; an encounter failure with dependent orders; certificate/token expiry; restore with a source-replay gap; and two simultaneous incidents. For each: record trigger, expected alert, owner reached, allowed recovery, actual result, reconciliation and sign-off.

Security and exit are acceptance gates

Document subcontractor locations, approved access paths, revocation, evidence access and data return. Distinguish operational updates, security-incident reports and breach notifications under the BAA; involve privacy/legal owners. Agree who authorizes containment versus clinical continuity. On exit, export mappings, configurations, runbooks and incident history; transfer secret ownership securely and revoke departing access.

Sources and evidence boundaries

[1] ASTP/ONC: SAFER guides

[2] Google SRE: implementing SLOs

[3] HL7 v2.5.1: control and acknowledgments

[4] HL7 FHIR R4: RESTful API

[5] AWS: retry with backoff

[6] HHS: HIPAA and cloud computing

[7] NIST SP 800-34 Rev. 1: contingency planning

[8] NIST SP 800-66 Rev. 2: HIPAA implementation

[9] BLS: employer compensation costs

[10] NextGen: Mirth enterprise licensing

[11] FinOps Foundation: forecasting

[12] NIST SP 800-61 Rev. 3: incident response

[13] Google SRE: on-call staffing assumptions

[14] BLS: systems administrator salary benchmarks

[15] Google SRE: alerting on SLOs

[16] HHS: current Security Rule summary

The six-year HIPAA documentation rule does not impose a universal six-year payload retention period. Set payload and audit retention with privacy and records-management owners. Proposed regulatory changes must not be represented as current obligations.

CAPMINDS

Make the next decision with evidence

A managed service should survive a difficult test

Before signing a multi-year agreement, ask the proposed operator to walk through a lost acknowledgment, a failed encounter dependency and two concurrent incidents. Require the team to identify who acts, what can be replayed, where approval is needed and how successful delivery will be proven. The answers reveal more than a coverage-hours claim.

Work with CapMinds on integration operations

CapMinds can help assess healthcare integration workflows, monitoring gaps and recovery readiness across EHR interfaces, HL7/FHIR connections and integration-engine operations. Start with a bounded test-data workflow or interface pilot and use its findings to define the operating scope.

Bring to the discussion	Proposed working output
Interface inventory and priorities	A service boundary with owners and delivery evidence
Recurring incidents and recovery concerns	Monitoring gaps and one recovery runbook to validate
Coverage expectations and existing costs	An assumption register and scope-based five-year comparison

Agree pilot scope and deliverables before work begins. Production access, service-level commitments, coverage arrangements and prices belong in a reviewed statement of work; this playbook does not establish those commitments.

Review your integration operations with CapMinds

BOOK AN INTEGRATION OPERATIONS DISCUSSION

Start with one workflow. Establish its delivery evidence, recovery authority and operating cost. Expand coverage when the acceptance tests demonstrate that the service is ready.