Kinometric LLC — HIPAA Incident Response Tabletop Exercise

Kinometric LLC — HIPAA Incident Response Tabletop Exercise

Purpose: Satisfy the testing requirement of the HIPAA Security Incident Response Plan §12 and HIPAA Security Rule §164.308(a)(8) (Evaluation). This is a *production-gating item* — the completed record (Part 3 below) must exist before production athena go-live with the first practice.

Document version: 1.0 — created 2026-05-22 **Owner:** Anant Johnson, Security & Privacy Officer **Related:** `incident_response_plan.md` §12, `hipaa_breach_response.md`, `hipaa_risk_assessment.md` **Retention:** The completed record is retained for 6 years per §164.316.

This document has three parts: - **Part 1 — Logistics & setup** (read before the meeting) - **Part 2 — Facilitator script** (run during the meeting; ~60 minutes) - **Part 3 — Exercise record** (fill in during/after the meeting; this is the auditable artifact)

Part 1 — Logistics & Setup

Attendees (required quorum)

Per IR Plan §12, the exercise needs at minimum:

Role	Name	Present?
Security & Privacy Officer (facilitator)	Anant Johnson	☐
Managing Member / Executive Sponsor	Steve Johnson	☐
Kinometric workforce member with PHI access (≥1)	_____	☐

Optional but recommended: Technical Lead (Charlie Rogers).

Before the meeting

- Facilitator confirms the quorum above is scheduled for a ~75-minute block (60 min exercise + 15 min buffer).
- Each attendee has a copy of `incident_response_plan.md` open or printed.
- Facilitator has this document; only the facilitator reads the **injects** ahead of time. Other attendees should *not* pre-read Part 2 — the value is in working the Plan live.

- No production system is touched during the exercise. This is a discussion-based (talk-through) tabletop, not a live drill.

Ground rules (facilitator states these at the start)

1. This is a no-fault exercise. “I don’t know where that is in the Plan” is a finding, not a failure — it is exactly what we are here to surface.
2. Answer from the Plan as written, not from what we *intend* to do. If the Plan is silent or ambiguous, say so — that becomes a corrective action.
3. The facilitator captures every gap, ambiguity, and missing contact in Part 3 as we go.
4. Timekeeping: the facilitator moves the group along; deep tangents are parked in the “Gaps / parking lot” list.

Part 2 — Facilitator Script (~60 minutes)

Scenario (the IR Plan §12 reference scenario)

> **It is 08:15 on a Tuesday.** The first item in the overnight athena integration audit log shows **50 GET /patients/{id} lookups between 02:00 and 02:40, all from a single IP address that does not match the production Linode host or any known Kinometric admin IP.** The Operations distribution channel (`dev@kinometric.com`) received an automated security alert about the pattern at 02:41; nobody saw it until the Security Officer opened email at 08:15.

The facilitator presents the scenario above, then works the five segments below. Each segment maps to a section of the IR Plan. Capture findings in Part 3 continuously.

Segment 1 — Detection & Reporting (~8 min) — IR Plan §4, §5

Ask the group:

1. Which detection source caught this? Is that source one we actually have configured and monitored today, or aspirational? *(Verify against §4 Detection Sources.)*
2. The alert sat unread for ~5.5 hours. Does the Plan set an expectation for how quickly the Operations channel is monitored? Is `dev@kinometric.com` monitored after hours? **If not — finding.**
3. Who formally “reports” this incident, to whom, and using what acknowledgment step? Walk through §5.

> **Inject 1a (facilitator reveals after initial discussion):** The IP geolocates to a country where Kinometric has no workforce and no subprocessor. Does that change anyone’s assessment?

Segment 2 — Triage & Classification (~12 min) — IR Plan §6

Walk the §6 classification flowchart out loud as a group:

1. Is this a security event? Is unauthorized access to PHI *suspected* or *confirmed* at this point?
2. What severity — S1, S2, S3? Justify against the §6 severity table. *(Expected reasoning: athena credential exposure suspected → S2; escalates to S1 if confirmed compromised. Capture whatever the group decides and the reasoning.)*

3. What is the classification deadline from §6, and the containment deadline for that severity? State the actual clock times.
4. Who owns the classification decision? Is that person available right now in the scenario?

> **Inject 2a:** While triaging, someone checks the athena Developer Portal and sees the API calls were authenticated with **Kinometric's production `client_secret`** — i.e., a valid credential, not a brute-force attempt. Re-run the classification. Does severity change? Does "suspected" become "confirmed"?

Segment 3 — Containment, Eradication, Recovery (~15 min) — IR Plan §7

With Inject 2a in force (valid credential used), walk §7:

1. Which "Standard containment actions" from §7 apply? Walk through the **athena API anomaly** and **suspected credential compromise** steps verbatim — can each person say *who* does it and *how*?
2. Rotate the athena `client_secret`: who has access to the athena Developer Portal? Where is the secret stored on the server, and how is it updated? *(Expected: encrypted at rest via `sodium_crypto_secretbox`, key at `/etc/kinometric/athena_key`; token cache at `/tmp/athena_token_cache_*.json` must be cleared.)* **If anyone in the room cannot name the portal owner — finding.**
3. How did the `client_secret` leak? Eradication: name the candidate root causes and how each would be investigated.
4. Recovery: what is the smoke test before athena calls resume? What does "14 days heightened monitoring" concretely mean here?

> **Inject 3a:** The athena Developer Portal account is owned by an individual whose login MFA device is unavailable this morning. How does the team rotate the secret anyway? **This is likely a finding — capture it.**

Segment 4 — Investigation & Breach Determination (~13 min) — IR Plan §6 risk assessment, §8, §9

1. 50 patient records were read by an unauthorized party. Walk the §6 risk-assessment branch: is the probability that PHI was compromised "low (documented)" or "more than low"? *(Expected: 50 confirmed PHI reads with a valid credential from an unknown IP → "more than low" → Confirmed Breach.)*
2. Once classified a **breach**, who must be notified, and on what clock? Walk §9 timing — practice (Covered Entity) notification, and the practice's downstream obligations to individuals and HHS.
3. **Critical role question:** Kinometric is the Business Associate. Who is the *formal notifier* to the 50 patients? *(Expected: the practice as Covered Entity; Kinometric drafts/supports per §9 and the BAA.)* Does everyone in the room understand that split?
4. Evidence preservation (§8): what gets preserved, where, and who maintains the investigation file?

> **Inject 4a:** The 50 records belong to patients of the *first deploying practice* — with whom the **BAA is not yet signed** (open item in `hipaa_risk_assessment.md` §4). The Plan's notification procedure assumes a signed BAA defines the notification timeline. What do we do? **Capture as a finding — this links breach readiness to the open BAA gap.**

Segment 5 — Documentation, Notification Content & Post-Incident (~10 min) — IR Plan §9, §10, §11

1. Open Appendix A (breach notification letter template). Could the team produce a compliant individual notice from it today? What fields would block us?
2. §10: where does the incident file live, who can access it, and what is the retention period?
3. §11 post-incident review: who runs it, on what timeline, and what triggers a Plan update?
4. Final sweep: list every contact field in the Plan that is still a placeholder (`NEEDS PHONE NUMBER`, Steve's contact details, etc.). Every one is a finding until filled.

Wrap-up (~2 min)

Facilitator reads back the findings list from Part 3 so the group agrees it is complete and accurate before adjourning. Each finding must have an owner and a target date.

Part 3 — Exercise Record (the auditable artifact)

> Fill this in during and immediately after the exercise. This completed section is the evidence that IR Plan §12 / §164.308(a)(8) is satisfied. Do not leave blanks — write "N/A" or "none" explicitly.

Exercise metadata

Field	Value
Date conducted	_____
Start / end time	_____
Format	Discussion-based tabletop (talk-through)
Facilitator	_____
Scenario used	athena audit log — 50 unauthorized /patients lookups overnight (Part 2)
IR Plan version exercised	v1.0 (2026-05-18)

Attendees

Name	Role	Quorum role satisfied

Decisions reached during the exercise

Segment	Decision (e.g. classification, severity, breach determination)	Rationale
2 — Classification		
2 — Severity		
4 — Breach determination		

4 — Formal notifier	

Findings — gaps, ambiguities, missing contacts

#	Finding	IR Plan section	Severity (H/M/L)	Corrective action	Owner	Target date
1						
2						
3						
4						
5						

Parking lot (items raised but out of scope for this exercise)

-

Plan changes triggered by this exercise

Per IR Plan §13, the Plan is reviewed after any tabletop. List the edits to `incident_response_plan.md` (or other docs) resulting from the findings above:

-

Sign-off

Role	Name	Signature	Date
Security & Privacy Officer	Anant Johnson	_____	_____
Managing Member	Steve Johnson	_____	_____

Production-gate status

☐ All findings have an owner and target date, and the IR Plan has been updated per §13. **The §12 tabletop production-gating item is satisfied** once this box is checked and the record is signed.

> After completion: update `incident_response_plan.md` §12 “Current status” to record the date this exercise was conducted, and file this completed record in the document retention system (6-year retention per §164.316).