

AI Incident Response Tabletop Exercise

Artifact 8 | NorthStar Health Network

NorthStar Health Network is a fictional regional health system comprising 12 hospitals, 70 outpatient facilities, approximately 18,000 employees, and roughly 3 million annual patient encounters. All systems, metrics, incidents, vendors, and findings in this portfolio are simulated.

Tabletop Scenario

Friday 07:30: A hospitalist reports that two deteriorating patients did not trigger expected sepsis alerts. At 08:05, analytics identifies a sharp decline in laboratory-interface completeness after a middleware update deployed overnight. One patient required ICU transfer. The model vendor also confirms a minor scoring-library update released two days earlier that NorthStar had not formally approved.

Exercise Objectives

- Detect and contain a potential AI-related patient-safety event.
- Separate data-pipeline failure from model-change risk.
- Test pause authority and clinical fallback workflow.
- Identify affected patients and review potential harm.
- Coordinate IT, vendor, clinical, privacy/security, legal, quality, and executive response.
- Preserve evidence and document reinstatement criteria.

Incident Response Sequence

Phase	Required actions	Lead
Detect / classify	Open AI incident; classify severity; verify clinical impact; preserve model/version/data logs	Patient Safety + Clinical AI Safety
Contain	Suppress unreliable scores; alert clinicians; activate manual deterioration workflow; freeze model/vendor changes	CMIO / Incident Commander
Scope	Identify affected sites, time window, patients, missing data elements, model versions	Analytics + IT
Investigate	Root-cause data pipeline, vendor change, thresholds, and workflow effects; assess PHI/security implications	Cross-functional incident team
Patient review	Review potentially affected charts; determine whether notification/remediation is needed	Quality / Clinical leadership
Correct	Restore validated feed; rollback or validate version; test end-to-end; retrain staff if workflow changed	IT + Model Owner
Reinstate	Document evidence; obtain required approval; enhanced monitoring period	Clinical AI Governance Committee
Learn	RCA, control changes, vendor remediation, lessons learned, board / committee reporting if material	Patient Safety + Risk

Key Exercise Decisions

Decision	Expected answer
Who can pause the model?	Designated clinical safety / CMIO / incident leaders without waiting for vendor permission.
What is the fallback?	Manual clinical deterioration and sepsis pathways remain available and are communicated immediately.
What evidence is preserved?	Model version, vendor release notes, interface logs, patient alerts, user actions, dashboard metrics, tickets, committee decisions.
What blocks reinstatement?	Unresolved patient-safety cause, incomplete end-to-end test, unapproved model version, missing subgroup/site validation, or inadequate clinician communication.

After-Action Findings

- Strength: NorthStar has rapid pause authority and an independent clinical fallback.
- Gap: Vendor change notification did not reliably trigger governance review.
- Gap: Data-interface health was monitored technically but not connected to model-safety suppression.
- Action: Create automated fail-safe suppression when required inputs breach freshness/completeness thresholds.
- Action: Add contract and technical controls requiring advance vendor change notice and version acceptance.