CASE STUDY

HEALTHCARE

Designing a Repeatable Incident Response Program for Healthcare Risk Preparedness

How a mid-sized healthcare organization built structured IR capability from the ground up, eliminating regulatory exposure and establishing durable readiness across clinical and administrative operations.

Kimly Hong

Cybersecurity and Information Security Leader

IAM | GRC | Incident Response | Risk Management

kimlyhong.com

Executive Summary

A mid-sized healthcare organization operating across multiple care delivery sites lacked formal incident response procedures, had never conducted structured tabletop simulations, and faced growing regulatory pressure under HIPAA and related frameworks. Audit findings had flagged the absence of documented escalation protocols and tested response workflows as a material compliance gap. The organization retained cybersecurity program leadership to design and operationalize an end-to-end incident response readiness program from the ground up.

The engagement produced a complete incident response playbook covering classification, escalation, containment, and recovery; a cross-functional escalation workflow matrix; a recurring tabletop simulation program; an incident classification taxonomy aligned to healthcare-specific threat categories; and a structured lessons-learned framework enabling continuous improvement after each simulation and real-world event.

Within twelve months the organization had conducted four facilitated tabletop exercises spanning clinical, administrative, and technology teams; closed its outstanding audit findings in the incident response domain; and established a governance structure capable of sustaining program operations without ongoing external support. Post-engagement assessment confirmed improved cross-team escalation readiness and materially reduced regulatory exposure across the incident management control domain.

> **Engagement Snapshot**
>
> *Industry: Healthcare. Organization Profile: Multi-site, mid-sized care delivery and administrative operations. Primary Challenge: No tested incident response workflow, no simulation capability, active regulatory compliance pressure. Program Duration: Twelve months. Core Deliverables: IR Playbook, Escalation Workflow Matrix, Tabletop Simulation Program, Classification Taxonomy, Lessons-Learned Framework.*

Organizational Context

The organization provided care delivery and administrative health services across multiple regional sites, with a workforce that included clinical staff, information technology personnel, and administrative business units. Like many mid-sized healthcare operators, the organization had grown its technology footprint rapidly over the preceding several years through system modernization initiatives and expanded digital health capabilities. This growth introduced meaningful cybersecurity complexity that the existing operational procedures had not kept pace with.

Operating Environment

Clinical and administrative operations ran across a combination of on-premises infrastructure and cloud-hosted applications. Patient data resided across electronic health record systems, ancillary clinical platforms, and administrative databases, creating a broad and varied attack surface. Third-party vendors and technology partners accessed systems under varying levels of formal access governance, and the

organization's endpoint environment spanned managed devices in controlled settings and semi-managed devices in distributed clinical locations.

Technology and Compliance Profile

The organization operated under HIPAA Privacy and Security Rule requirements and maintained relationships with insurers and government payers that imposed contractual security obligations. Prior audit cycles had identified gaps in security awareness, access governance, and incident management readiness. The incident management gap was the most acute: documentation requirements under HIPAA's Breach Notification Rule and Security Rule mandated both a formal incident response procedure and evidence of its testing, neither of which the organization could demonstrate at the outset of the engagement.

Staffing and Governance Baseline

The information security function was staffed by a small team responsible for a broad portfolio of security operations, compliance, and technology risk activities. There was no dedicated incident response function, and no staff member had a clearly designated role in coordinating a security incident across organizational boundaries. Escalation decisions historically relied on informal communication channels and individual judgment rather than documented protocols, a pattern that created inconsistency and delayed containment in past minor incidents.

Risk Landscape

Healthcare organizations present a distinct and well-documented threat profile. Patient data carries significant value on illicit markets, clinical operations create pressure against service disruption that threat actors exploit, and the sector's technology environment is often more heterogeneous and harder to govern than comparably sized organizations in other industries. The risk landscape assessment at the outset of this engagement confirmed that each of these systemic factors was present and that the absence of a tested incident response program amplified exposure across all of them.

Ransomware and Operational Disruption

Healthcare has remained among the most heavily targeted sectors for ransomware due to the operational consequences of system unavailability in care delivery contexts. Without a tested incident response playbook and defined escalation procedures, the organization had no documented path from initial detection of a ransomware event to isolation, clinical workflow continuity, leadership notification, and regulatory reporting. The absence of tabletop exercises meant that staff had no practiced familiarity with their roles in such a scenario.

Phishing and Social Engineering

The organization had conducted phishing awareness training in prior periods, but the training program was not integrated with incident response procedures. Staff who identified a potential phishing attempt had no defined reporting pathway, and no procedure existed for escalating a suspected credential

compromise into a formal security investigation. This gap meant that early-stage incidents were likely going undetected or unreported, increasing the probability of escalation to a material breach before any coordinated response could begin.

Third-Party and Vendor-Initiated Risk

Vendor and partner access to clinical and administrative systems was governed inconsistently, and no procedure existed for incorporating a third-party-involved incident into the organization's response workflow. Scenarios involving a compromised vendor credential, a supply chain software event, or a business associate data exposure were entirely outside the scope of existing informal escalation practices, creating a class of incident for which the organization had no response capability at all.

Regulatory and Reporting Exposure

HIPAA's Breach Notification Rule requires covered entities to notify affected individuals, the Department of Health and Human Services, and in some cases media outlets within defined timeframes following the discovery of a breach involving unsecured protected health information. These reporting obligations run from the date of discovery, not the date of containment. Without a tested incident response procedure that defined discovery, classification, and escalation roles, the organization faced a meaningful risk of missing reporting deadlines simply due to organizational confusion in the immediate aftermath of an incident.

Risk Category	Observed Condition	Program Implication
Ransomware / Disruption	No isolation or continuity procedure documented or tested	Playbook and tabletop simulation required
Phishing / Credential Compromise	No staff reporting pathway; no escalation trigger defined	Classification taxonomy and escalation matrix required
Third-Party / Vendor Events	No vendor-specific response track; no partner notification procedure	Playbook scope expansion; vendor scenario tabletop required
Regulatory Reporting	No defined discovery-to-notification workflow; reporting timelines at risk	Escalation matrix and classification taxonomy required
Cross-Team Coordination	No documented escalation path; informal channels only	Roles and responsibilities definition required across program

Assessment Findings

A structured assessment was conducted at the outset of the engagement to establish baseline capability across four incident response competency domains: procedural documentation, escalation and coordination, simulation and testing, and regulatory alignment. Findings were rated across three levels: absent (no capability or documentation existed), informal (ad hoc or undocumented practice existed), and partial (documentation or practice existed but was incomplete or untested). No domain was rated capable at engagement initiation.

Finding 1: No Tested Incident Response Workflow

The organization had no documented incident response procedure of any kind. There was no playbook, no defined workflow from detection to containment, and no documented recovery procedure. Informal practices had developed over time within the technology team, but these were undocumented, inconsistently applied, and unknown to clinical and administrative business units. Rating: Absent.

Finding 2: Poor Cross-Team Escalation Readiness

Escalation decisions in prior incidents had been made informally by the individual who happened to be aware of the event, with no defined criteria for when an incident required leadership notification, legal involvement, or regulatory reporting. Clinical unit managers, HR, legal counsel, and communications had no defined role in any incident response scenario. Rating: Absent.

Finding 3: No Simulation Capability

The organization had never conducted a structured tabletop exercise or incident simulation of any kind. Staff in IT, clinical operations, and administration had no practiced experience with their roles in an incident scenario. There was no mechanism for identifying gaps in response capability before a real event, and no structured process for capturing lessons after a real or simulated event occurred. Rating: Absent.

Finding 4: Regulatory Compliance Pressure

Audit findings from the prior compliance cycle had flagged the absence of a documented and tested incident response procedure as a control deficiency under the HIPAA Security Rule. The organization faced a deadline for remediation documentation in the upcoming audit period. Separately, the organization's cyber liability insurer had requested evidence of incident response planning as a condition of coverage renewal, adding additional urgency to program buildout. Rating: Absent, with active compliance deadline.

Assessment Summary

Competency Domain	Baseline Rating	Primary Gap	Priority
IR Workflow	Absent	No playbook; no documented procedure	Critical
Escalation Readiness	Absent	No defined roles; no escalation criteria	Critical
Simulation Capability	Absent	No tabletop program; no lessons-learned process	High
Regulatory Alignment	Absent	Active audit finding; insurer requirement pending	Critical

Strategic Approach

The program was designed around three governing principles derived from the assessment findings. First, documentation and testing had to proceed in parallel rather than sequentially. An untested playbook would not satisfy the regulatory deadline or provide genuine operational readiness; the testing program had to begin as soon as a workable draft existed, with findings used to refine the playbook iteratively. Second, the program had to be cross-functional from the start. Incident response that exists only inside the technology team fails at exactly the moment a real incident requires organizational coordination. Clinical leadership, legal, HR, and communications were included in design, not just execution. Third, sustainability required a governance model that the organization could operate independently. External program design that requires ongoing external facilitation does not produce durable readiness.

Playbook-First Sequencing

The incident response playbook was developed as the foundational deliverable because every other program component depended on it. The playbook established the incident classification taxonomy, defined roles and responsibilities across functional units, specified notification and escalation criteria at each severity tier, and documented containment and recovery procedures for the most probable incident categories. A functional draft was completed within the first eight weeks, enabling tabletop planning to begin before the playbook was finalized.

Scenario-Driven Simulation Design

The tabletop simulation program was designed around the specific threat scenarios identified in the risk landscape assessment rather than generic incident response exercises. Each of the four annual simulations was mapped to a distinct scenario category: ransomware and operational disruption, phishing-initiated credential compromise, third-party vendor event, and regulatory reporting under compressed timelines. This scenario mapping ensured that the simulation program addressed the organization's actual risk profile rather than providing generic tabletop experience.

Cross-Functional Inclusion

Each tabletop exercise was structured to require active participation from clinical operations, IT, legal, HR, and communications alongside the security team. Scenario design was calibrated to surface the specific decision points where cross-functional coordination was most critical, including patient safety communications, media and public relations considerations, and regulatory notification timing. Functional leaders who had never been involved in a security exercise were introduced to the program through pre-exercise briefings that oriented them to their roles without providing answers to the scenario questions.

Governance and Continuity Design

A program governance model was established to ensure that incident response readiness did not decay between exercises or following personnel changes. The model defined an Incident Response Steering Committee responsible for annual playbook review and program oversight, an Incident Response Coordinator role within the security function responsible for exercise facilitation and playbook

maintenance, and an Incident Classification Board responsible for severity determination and escalation decisions during a live event. Documentation standards, evidence production requirements, and the annual simulation schedule were embedded in the governance model to produce continuity independent of individual personnel.

Implementation Roadmap

The program was executed in four phases over twelve months. Each phase produced concrete deliverables and was designed to build directly on the prior phase, ensuring that documentation, simulation, and governance capability developed in sequence without gaps in coverage.

Phase	Focus	Timeline	Primary Deliverable
Phase 1	Assessment, playbook development, classification taxonomy	Months 1-3	Incident Response Playbook v1.0; Classification Taxonomy
Phase 2	Escalation matrix design; first tabletop simulation	Months 3-6	Escalation Workflow Matrix; Tabletop 1 (Ransomware Scenario)
Phase 3	Playbook refinement; second and third tabletop simulations	Months 6-10	Playbook v2.0; Tabletop 2 (Phishing/Credential); Tabletop 3 (Vendor Event)
Phase 4	Governance model buildout; fourth tabletop; lessons-learned framework	Months 9-12	Governance Model; Tabletop 4 (Regulatory Reporting); Lessons-Learned Framework

Phase 1: Foundational Documentation

Phase 1 focused on building the documented foundation the simulation program would require. The incident response playbook was drafted through structured working sessions with the security team, technology leadership, and representatives from clinical operations and legal. The classification taxonomy was developed concurrently, establishing four severity tiers mapped to the organization's specific operational and regulatory context. By the end of Phase 1, the organization had a functional playbook and taxonomy; had identified the roles required for the escalation matrix; and had selected the scenarios for the first two tabletop simulations.

Phase 2: Initial Simulation and Escalation Design

Phase 2 introduced structured testing alongside the escalation matrix development. The escalation workflow matrix was completed in the first weeks of Phase 2 and immediately incorporated into tabletop planning. The first tabletop simulation, built around a ransomware scenario affecting clinical systems, was facilitated in Month 5. Participation included clinical operations, IT, legal, and communications. Post-exercise debrief produced a structured findings report, and the highest-priority gaps were incorporated into the Phase 3 playbook revision.

Phase 3: Iterative Refinement

Phase 3 applied the lessons from the first simulation to a revised playbook and conducted two additional exercises. The phishing and credential compromise scenario surfaced gaps in the organization's user notification and account revocation procedures that were not visible in a ransomware scenario. The vendor event tabletop introduced the organization's legal and compliance functions to third-party notification requirements and produced revisions to the playbook's vendor-incident track. By the end of Phase 3, the playbook had been tested across three distinct scenario types and refined based on structured exercise findings.

Phase 4: Governance and Sustainability

Phase 4 established the governance model and conducted the final tabletop simulation, which tested regulatory reporting procedures under a compressed timeline scenario. The governance documentation defined the Incident Response Steering Committee charter, the Coordinator role responsibilities, and the annual exercise calendar. The lessons-learned framework was finalized and integrated into the post-exercise documentation standard. At program close, all regulatory audit findings in the incident response domain were closed, and the organization could demonstrate a tested, documented, and governed IR program to its insurer and auditors.

Governance Model

The governance model was designed to maintain incident response readiness as a durable organizational capability rather than a project-era artifact. Three governance tiers were established, each with defined membership, decision authority, and accountability. The model was documented in the playbook and in a separate governance charter, and onboarding materials were prepared to orient new members of each tier to their responsibilities.

Strategic Tier: Incident Response Steering Committee

The Incident Response Steering Committee was composed of the Chief Information Officer, Chief Compliance Officer, General Counsel, and the senior leader responsible for clinical operations. The committee met annually to review and approve updates to the incident response playbook, review the prior year's simulation findings and remediation progress, approve the upcoming year's simulation calendar and scenario selections, and assess the organization's overall incident response posture against the regulatory and threat landscape. The committee also served as the organizational sponsor for any material investment in incident response capability or tooling.

Operational Tier: Incident Response Coordinator

The Incident Response Coordinator role was assigned to a senior member of the security function and carried responsibility for day-to-day program operations. Coordinator responsibilities included maintaining the playbook between annual reviews, facilitating the tabletop simulation program, tracking remediation of simulation findings, maintaining the evidence record required for regulatory and insurer

demonstration, and serving as the operational lead in the initial phase of a real incident before the Incident Classification Board convened.

Execution Tier: Incident Classification Board

The Incident Classification Board was a standing cross-functional group convened during a live incident to determine severity classification, authorize escalation decisions, and coordinate response across functional units. Standing members included the IT Security Lead, Clinical Operations Representative, Legal Counsel, and HR Representative. Communications was included for any incident at Severity 2 or above. The board operated under documented decision criteria defined in the escalation workflow matrix, reducing the reliance on individual judgment under pressure.

Roles and Control Responsibilities

Role	Primary Responsibility	Key Controls Owned
IR Steering Committee	Strategic oversight; annual playbook approval; program sponsorship	Playbook review and approval; annual exercise authorization; posture assessment
IR Coordinator	Operational program management; tabletop facilitation; evidence maintenance	Playbook currency; simulation calendar; remediation tracking; regulatory evidence
Incident Classification Board	Live incident severity determination; cross-functional escalation coordination	Severity classification; escalation authorization; containment decision
Clinical Operations Representative	Clinical workflow continuity; patient safety communications	Clinical impact assessment; care continuity protocol activation
Legal Counsel	Regulatory notification determination; breach assessment	HIPAA notification timeline; legal hold; third-party notification

Outcomes

Program outcomes were assessed at twelve months against the four competency domains identified in the baseline assessment. In each domain, the organization moved from an absent or informal capability to a documented, tested, and governed program. Regulatory findings were closed, insurer requirements were satisfied, and operational readiness was measurably improved.

Incident Response Workflow

The organization completed the engagement with a fully documented incident response playbook covering six distinct incident categories: ransomware and destructive malware, phishing-initiated credential compromise, unauthorized access and insider threat, third-party and vendor-initiated events, data exposure and potential breach, and system availability events affecting clinical operations. Each playbook track included detection criteria, initial response steps, escalation triggers, containment and

recovery procedures, and regulatory notification guidance. The playbook had been tested across four tabletop scenarios and revised through two formal version cycles.

Escalation Readiness

The escalation workflow matrix established defined escalation paths for each severity tier, with documented criteria for when clinical leadership, legal, HR, communications, and executive leadership entered the response workflow. Post-program tabletop debrief scores on escalation decision quality improved substantially from the first to the fourth simulation, reflecting the practical familiarity developed through repeated exercise. Cross-functional participants who had never been involved in a security scenario reported confidence in their incident role by the program's final exercise.

Simulation Capability

The tabletop simulation program was fully operational at program close, with an annual four-exercise calendar, scenario selection criteria, facilitation materials, and a standardized post-exercise debrief and findings documentation process. The lessons-learned framework ensured that each simulation produced actionable remediation items tracked through to closure. The organization had the internal capability to facilitate future exercises without external program support, supported by the documented simulation program design and facilitator guidance materials developed during the engagement.

Regulatory and Compliance Outcomes

All outstanding audit findings in the incident response domain were closed prior to the annual compliance review. Documentation submitted to the auditor included the incident response playbook, the classification taxonomy, the escalation workflow matrix, the four tabletop exercise reports, and the remediation tracking record. The cyber liability insurer accepted the program documentation as satisfying its incident response planning requirement, and coverage was renewed without condition. No exceptions in the incident response domain appeared in the post-program audit cycle.

Outcome Summary

Domain	Baseline State	Post-Program State
IR Workflow	Absent; no documented procedure	Complete playbook across six incident categories; tested and version-controlled
Escalation Readiness	Absent; informal channels only	Documented matrix; defined roles; cross-functional familiarity confirmed through four simulations
Simulation Capability	Absent; no exercises conducted	Annual four-exercise program; facilitator materials; lessons-learned framework operational
Regulatory Alignment	Active audit finding; insurer condition outstanding	All findings closed; insurer requirement satisfied; no exceptions

Domain	Baseline State	Post-Program State
		in post-program audit
Governance	No IR governance structure	Three-tier governance model; annual charter; coordinator role assigned and operational

Lessons Learned

Programs of this kind produce lessons that extend well beyond the specific organizational context. The following reflections are offered for healthcare security leaders and operational executives considering a similar incident response buildout.

Documentation and Testing Must Run in Parallel

A common pattern in incident response program design is to complete the playbook before beginning simulation work, on the theory that staff cannot be tested against a procedure that does not exist. In practice, this sequence wastes the most valuable learning the simulation program has to offer. A functional draft playbook is sufficient to run a tabletop exercise, and the gaps that exercise reveals are more likely to be real gaps than anything a desk review of the draft would surface. Beginning simulation work before the playbook is finalized means the playbook reflects tested, not theoretical, procedure from its first version.

Cross-Functional Inclusion Is the Program, Not an Add-On

Healthcare incident response fails most visibly at the intersection of clinical operations, legal, communications, and security. Technology teams can execute excellent containment work while clinical leadership, legal, and communications remain unaware of the event or uncertain of their roles. Designing the simulation program to require meaningful participation from non-technology functions is not a complexity burden; it is the point of the exercise. The first tabletop session that brings clinical and legal participants into an IR scenario together is more valuable than any number of technology-only exercises.

Severity Taxonomy Drives Every Downstream Decision

Every downstream element of an incident response program, escalation criteria, notification requirements, containment authority, regulatory reporting obligations, depends on a shared understanding of incident severity. Organizations that skip or defer the classification taxonomy work discover this during exercises when participants disagree about what a given scenario requires. Developing the taxonomy before the escalation matrix and before the first tabletop exercises meant that every subsequent program element rested on a shared definitional foundation.

Regulatory Deadlines Can Be Used as Program Anchors

The active audit finding at the outset of this engagement created organizational urgency that might otherwise have been difficult to sustain across a twelve-month program. Rather than treating the deadline

as an obstacle, the program design used it as an anchor. The first-phase playbook and taxonomy deliverables were sequenced to produce documentation satisfying the most urgent regulatory requirement before the simulation program had fully matured. This protected the organization's compliance posture while preserving the time needed to build genuine readiness.

Sustainability Requires Governance Before It Requires Expertise

Organizations that build incident response programs around individual expertise rather than documented governance find that readiness is tied to specific personnel. When those personnel transition, readiness erodes. The governance model established in Phase 4 was designed explicitly to be operated by capable but not expert practitioners, with documented decision criteria, a maintained evidence record, and a facilitation guide for the simulation program. The goal was a program that a new IR Coordinator could inherit and operate without needing to rebuild from the prior coordinator's institutional knowledge.

> **Closing Reflection**
>
> *Incident response readiness in healthcare is not primarily a technology problem. It is an organizational coordination problem that technology events expose. Programs that treat IR as a security team responsibility consistently underperform when real incidents require clinical, legal, and communications coordination under pressure. Organizations that build cross-functional readiness through structured simulation, and govern that readiness through documented roles and recurring exercises, are better positioned to contain incidents quickly, satisfy regulatory obligations, and protect patient trust.*

About the Author

Kimly Hong is a cybersecurity and information security leader with more than a decade of experience driving enterprise security programs across financial services, gaming and hospitality, and investment management. She has led identity and access management modernization for global application portfolios, directed privileged access governance programs across multi-property enterprises, and coordinated incident response readiness initiatives at the enterprise level.

Her professional background includes enterprise cybersecurity program management at a multi-property gaming and hospitality operator, information security program leadership at a regional commercial bank supporting IAM across dozens of global applications, and information security team leadership at a major investment management firm. She holds an MBA in Strategic Leadership from Bryant University, a Bachelor of Science in Management of Information Systems from Husson University, and the Certified ScrumMaster (CSM) credential.

Kimly advises mid-size and enterprise organizations on cybersecurity program design, identity governance, privileged access management, incident response readiness, and regulatory alignment across HIPAA, SOX, GLBA, PCI DSS, and related control regimes. Her advisory practice focuses on organizations that need to build or rebuild core security program capability without disrupting operations.

Contact and additional case studies: kimlyhong.com