Healthcare Cyber Risk Advisory

8-WEEK ASSESSMENT BOARD-READY OUTPUT POST-CHANGE HEALTHCARE ERA

After Change Healthcare, cyber risk became a board-level conversation at every health system. A3HCS delivers an 8-week independent assessment that surfaces vendor concentration risk, third-party exposure, and HIPAA security gaps, and ships a 12-month remediation roadmap your board can approve and your CIO can execute.

100M+	$2.5B+	8 weeks
AMERICANS EXPOSED, CHANGE HEALTHCARE	REMEDIATION COST, ONE OPERATOR	DIAGNOSTIC TO BOARD-READY PLAN

Industry reference points. Engagement scope and target outcomes calibrated to facility size and risk posture.

THE PROBLEM

Most healthcare cyber assessments are vendor scorecards. They tell you which tools you have. They do not tell you whether you would survive a Change Healthcare-style outage. The wrong question, even when answered well, produces the wrong plan.

Third-party concentration risk is invisible. Most health systems do not know how many critical clinical workflows depend on a single vendor until that vendor goes down. By then the outage is the assessment.

HIPAA Security Rule is tightening. OCR enforcement has sharpened. Hospitals are caught between an older standard and rising expectations, often without a clear view of where the gap actually is.

Boards are asking questions IT cannot answer. The board wants risk in dollar terms, in patient terms, and in continuity terms. IT speaks in CVE numbers and tool inventories. The translation is the missing layer.

THE A3HCS SOLUTION

An 8-week independent cyber risk assessment that produces a board-ready risk report, a vendor concentration audit, and a 12-month prioritized remediation roadmap. Built by a physician-executive who understands clinical workflow continuity.

- **Asset and vendor inventory.** Weeks 1 to 2. Catalog of critical systems, third-party dependencies, and the clinical workflows they serve. Concentration-risk scoring per vendor.
- **Threat and continuity assessment.** Weeks 3 to 4. Business impact analysis. What breaks first if Change Healthcare happens here, what the patient impact looks like, and how long the operational fallback holds.
- **HIPAA Security Rule gap analysis.** Weeks 4 to 6. Mapping against OCR enforcement priorities and current minimum expectations. Identification of high-risk gaps by domain.
- **Remediation roadmap and board memo.** Weeks 7 to 8. 12-month plan with budget ranges, sequencing, and board-readable framing. Optional quarterly board cadence available after handoff.

THE 5-DOMAIN HOSPITAL CYBER RISK MAP

Most assessments cover one or two domains and call it done. A3HCS covers all five because a board-level answer requires all five.

DOMAIN	NAMED OWNER	WHAT WE REVIEW
1. Critical System Inventory	CIO / CISO	EHR, RCM, lab, imaging, scheduling, claims clearinghouse. Single points of failure mapped.
2. Third-Party Vendor Exposure	CIO / Supply Chain	Vendor concentration, contract continuity clauses, SLA enforcement, BAA coverage.
3. HIPAA Security Rule Readiness	Compliance / CISO	Administrative, physical, technical safeguards. OCR enforcement priorities.
4. Clinical Continuity Planning	COO / CMIO	Downtime protocols, paper-based fallback, clinical decision support without EHR access.
5. Board & Executive Reporting	CISO / CIO / CEO	Risk in dollar and patient terms. Quarterly cadence. Audit-defensible.

THE 8-WEEK ENGAGEMENT

Phase 1, Inventory
WEEKS 1 TO 2

Asset catalog. Vendor map. Concentration scoring.

Phase 2, Assess
WEEKS 3 TO 6

Continuity analysis. HIPAA gap analysis. Patient-impact modeling.

Phase 3, Plan
WEEKS 7 TO 8

12-month roadmap. Board memo. Budget ranges. Sequencing.

ENGAGEMENT & WHY A3HCS

Engagement Structure

Fixed-fee, scoped per facility size and vendor stack complexity. Three-phase delivery over 8 weeks.

DELIVERABLES

Critical asset inventory, third-party vendor concentration audit, continuity and patient-impact analysis, HIPAA Security Rule gap analysis, 12-month prioritized remediation roadmap, board-ready briefing memo.

Optional quarterly board-reporting retainer available after the assessment. Keeps the risk register current and audit-defensible.

Why A3HCS

Independent of your cyber vendor stack. We do not sell tools. We are not a managed security provider. The recommendation is the deliverable, not a sales motion.

Patient impact framing, not CVE counts. The board wants risk in patient and continuity terms. We deliver it that way.

Built from inside the hospital. Continuity planning is operational, not just technical. A physician-executive lead changes the assessment quality.

Post-Change Healthcare framing. Concentration risk and third-party exposure are now first-class assessment dimensions, not footnotes.

Schedule a Strategy Consultation

30-minute call to assess fit, baseline opportunity, and engagement scoping. No obligation. • **a3hcs.org** •

Nitesh Kumar, MD, MBA, ACHE, Six Sigma Black Belt