

Cyber Resilience for Healthcare Organizations

Overview

When disruption hits, the question your board asks is not “Were we breached?” It is “Can we still deliver care?” Meditology helps healthcare organizations stay operational, recover faster, and keep patient care moving with a resilience program built around your clinical and business workflows.

Your board does not want a list of unpatched servers. It wants to know whether the organization can continue treating patients through ransomware attacks, a cloud outage, or the failure of a critical vendor. Most security programs cannot answer that question because they are built around controls and frameworks instead of the workflows that keep the organization running.

When leadership receives disconnected findings from different functions using different metrics and severity scales, it becomes difficult to understand the organization’s true exposure. Business impact—not technical findings—gives executives the context needed to make informed decisions. In healthcare, downtime, diversion, and vendor failure put patient safety and organizational trust at risk.

Cyber Resilience reframes the program around the workflows that keep care moving and the security capabilities that protect them.



Four Practice Pillars



Resilience Alignment

We map critical security functions to the clinical and business workflows they protect, then build a board-ready resilience narrative. You see security expressed in business outcomes, not control checklists.



Maturity Assessment

We benchmark your resilience against the National Institute of Standards and Technology Cybersecurity Framework 2.0 (NIST CSF 2.0, with emphasis on Govern, Identify, Recover), HITRUST resilience domains, and HIPAA contingency requirements, with healthcare peer context plus technical Recovery Capability Validation. You get a defensible current-state picture.



Vendor Resiliency

We map vendor dependencies to workflows, tier them by impact, and expose concentration and fourth-party risk through our Critical Vendor Risk Intelligence (CVRI) methodology. You see your true vendor blast radius.



Tabletop Testing

We stress-test your response and recovery plans with healthcare-realistic, scenario-driven exercises, available one-time or as an annual program. You experience how your team performs before a real incident tests it.

Our Approach: How It Works

Resilience is treated as an operating model—a continuous cycle of identifying critical processes, mapping security to business outcomes, testing recovery, and adapting—not a project with a completion date. The practice is structured as four pillars, each available standalone or sequenced into an integrated program.

What You Get

Concrete deliverables across the practice, named as you receive them:

- Resilience mapping model and security-to-resilience traceability matrix
- Gap analysis and prioritized remediation roadmap
- Board-ready executive summary deck and resilience narrative
- Current-state maturity scorecard with healthcare peer context and framework cross-walk
- Vendor dependency map, concentration and fourth-party risk register, and blast-radius assessment
- Tabletop scenario package, after-action report, and corrective-action register

Typical Timeline

Individual pillar engagements run roughly 2 to 12 weeks each depending on the service. A typical integrated assessment engagement runs 16+ weeks depending on stakeholder responsiveness.

Who is Involved

Meditology's team includes an engagement lead, resilience consultants, healthcare CISO advisors for executive framing and tabletop facilitation, and risk analysts.



Why Meditology

Meditology is a healthcare-exclusive cybersecurity, privacy, risk, and compliance firm operationalizing GRC across your enterprise. Meditology, powered by CORL Technology, performs 8,000+ vendor assessments per year, the operational depth behind our Vendor Resiliency analysis. For Cyber Resilience, three things matter most:



Plug-in

We integrate with your existing frameworks, platforms, and workflows. No rip-and-replace. We operationalize findings into owned action items, SLAs, due dates, dashboards, and audit-ready reporting, elevating what you already have.



Purpose-built

Designed for healthcare complexity: clinical and operational dependencies (care comes first), expansive vendor ecosystems, medical device risk, and lean security teams. Our Critical Vendor Risk Intelligence (CVRI) methodology, powered by CORL, maps your vendor blast radius across an ecosystem informed by 80,000+ vendors in our CORL data.



Integrated

GRC enablement connects services across disciplines. Vendor risk integrates into organizational governance, and compliance programs strengthen resilience planning. Vendor risk integrates into organizational governance.

About Meditology

Meditology helps healthcare organizations turn cybersecurity, risk, and compliance into a strategic advantage, integrating deep healthcare expertise, end-to-end delivery, and tailored solutions to increase operational resilience and business value.

Build the resilience your organization needs to keep patient care moving.

Talk to a healthcare cybersecurity expert today.



MEDITOLOGY
SERVICES

Copyright © 2026 Meditology Services. All rights reserved.