

Protecting Patient Data from Cyber Threats in Healthcare

A 7-Step Framework for Healthcare Security

Cybersecurity isn't just a technical function, it's a strategic imperative that protects patients, preserves care continuity, and strengthens organizational resilience. Stronger cybersecurity starts with smarter data and integrated risk management. Ready to elevate your defenses? Contact our experts to build an integrated risk management approach that safeguards patient data today and prepares your organization for what's next.

STEP 1 Know Your Risk Landscape

Map where threats originate, including third-party vendors, to understand risk exposure across your entire ecosystem.



STEP 2 Build Unified Risk Management

Establish an integrated risk management framework that aligns IT, compliance, clinical leadership, and vendor oversight.



STEP 3 Accelerate Assessments with AI

Use automated, AI-driven tools to rapidly assess security posture and prioritize the most critical risks in real time.



STEP 4 Strengthen Vendor Risk & Monitoring

Onboard vendors using tiered risk assessments, enforce contractual controls, and maintain continuous visibility into vendor security.



STEP 5 Plan for Continuity & Impact

Conduct business impact analyses to identify mission-critical systems and ensure care delivery continues during disruptions.



STEP 6 Leverage Analytics for Smarter Decisions

Apply advanced analytics to unify fragmented data environments and guide modernization, investment, and security priorities.



STEP 7 Embrace AI & Emerging Technologies

Deploy AI for adaptive threat detection and predictive defense while preparing for future innovations such as advanced threat models and blockchain.

