



Cyber Insurance Prep for Healthcare

Most healthcare providers fail their first cyber insurance submission. Here's how to avoid delays, denials, or higher premiums.

Why 70% of SMBs Fail Their First Submission



No clear logging of user/system activity



MFA in place, but not enforced consistently



Incomplete inventory of systems and data



Weak documentation around controls and backups

Every cybersecurity investment should protect your operations, your patients, and your reputation. This short review maps your current spending against what insurers, regulators, and attackers actually care about. You'll walk away with a risk-adjusted budget view—without needing to inventory every tool.

Contact Us:

 protectthecube.com

 info@protectthecube.com

 888-408-CUBE



Top 3 Missing Readiness Elements



Logging & Evidence

Insurers want to see centralized logging with alerting and retention policies. Without it, there's no proof of enforcement.



MFA Enforcement Scope

MFA must apply across staff, admins, cloud platforms, and legacy apps—not just a subset of users.



Asset Visibility

Without a live inventory of endpoints, cloud accounts, and mobile access, insurers can't assess your real risk.

How Cube IT Helps You Prepare



We provide audit-ready documentation bundles



Our SecureStart Assessment flags issues before your broker does



We work with your broker or insurance contact directly



Trusted by clinics, therapists, dental offices, and outpatient groups



Real-World Examples



Therapy Practice

Closed four readiness gaps in 30 days and passed on first submission.



Dental Office

Added missing MFA enforcement and device logging—qualified for a lower premium.



Outpatient Clinic

Used Cube IT's audit-ready bundle to simplify insurance renewal with zero back-and-forth.

Contact Us:



protectthecube.com



info@protectthecube.com



888-408-CUBE