MERIPLEX

Hospital Managed IT Provider Evaluation Scorecard

Risk Category	Key Signal to Listen For	Status
HIPAA Documentation	Describes BAA obligations operationally, addresses subcontractor PHI, names specific controls — not just 'we sign BAAs'	☐ Strong | ☐ Partial | ☐ Weak
	Describes a structured SRA methodology with ePHI flow mapping, risk levels, remediation roadmap, and offers a sample deliverable	☐ Strong | ☐ Partial | ☐ Weak
	Maintains written documentation, names policies and audit log retention practices, has a real OCR investigation reference	☐ Strong | ☐ Partial | ☐ Weak
Cybersecurity	Names the SIEM platform, describes healthcare-specific detection rules, explains escalation path to clinical leadership — not just IT	☐ Strong | ☐ Partial | ☐ Weak
	Provides healthcare-segmented MTTD/MTTR metrics — not blended across industries; benchmarks against NIST CSF	☐ Strong | ☐ Partial | ☐ Weak
	Describes network segmentation for clinical device VLANs, names passive monitoring platforms (Claroty, Medigate, Armis), explains biomedical coordination	☐ Strong | ☐ Partial | ☐ Weak
Ransomware Resilience	Produces an actual runbook with six documented steps covering isolation, forensics, clinical notification, downtime, legal, and breach timeline	☐ Strong | ☐ Partial | ☐ Weak
	Specifies immutable off-network backups, documented RPO/RTO per clinical system tier, quarterly restoration testing with shareable results	☐ Strong | ☐ Partial | ☐ Weak
	Describes a real healthcare incident — how they performed under operational pressure, what they changed — not just prevention messaging	☐ Strong | ☐ Partial | ☐ Weak
Subcontractor Accountability	Names the compliance owner by role and credentials (CISSP, CISA, CHPS), describes accountability continuity during staff turnover	☐ Strong | ☐ Partial | ☐ Weak
	Provides full subcontractor list, complete BAA chain, SOC 2 Type II for cloud/data center vendors — does not treat the question as unusual	☐ Strong | ☐ Partial | ☐ Weak
	Defines clinical impact event separately from standard IT outage; specifies response protocol tiers; answers what happens to patient care during an outage	☐ Strong | ☐ Partial | ☐ Weak