CloudWave

Managed Security Service Provider (MSSP) Evaluation Criteria

A Framework for Healthcare Organizations

Selecting an MSSP is one of the most consequential decisions a healthcare organization can make. The right partner understands your clinical environment, coordinates with your existing infrastructure, and makes containment decisions that account for patient safety. Use this framework to evaluate candidates across the dimensions that matter most.

Rate each vendor on a 1–5 scale (1 = Does not meet, 3 = Meets, 5 = Best in class) and compare weighted results.

Evaluation Criteria	What to Ask / Look For	Weight	Score
HEALTHCARE INDUSTRY EXPERTISE			
Healthcare Specialization	Is healthcare a primary focus, or one of many verticals? Ask what percentage of clients are healthcare.	High	
HIPAA & HITRUST Depth	Compliance expertise beyond a checkbox — BAA execution, audit support, policy alignment.	High	
Clinical Workflow Awareness	Can they distinguish clinical from administrative systems during detection? Do playbooks account for patient care impact?	High	
EHR Platform Knowledge	Experience with your EHR (MEDITECH, Epic, Cerner) — dependencies, traffic patterns, safe containment.	Med	
Medical Device Security	Ability to identify, monitor, and safely contain threats involving biomedical devices.	Med	
OPERATIONAL MODEL & ACCOUNTABILITY			
Direct SOC Relationship	Will you interact directly with monitoring analysts, or is there an intermediary (white-label, reseller, subcontractor)?	High	
Service Delivery Transparency	Can they identify who operates the SOC, where analysts are located, and the escalation path during a critical incident?	High	
Named Analyst Access	Can you meet the analysts monitoring your environment? Is there continuity in your assigned team?	Med	
INTEGRATION & UNIFIED VISIBILITY			
Infrastructure Integration	Can they extend protection across your full enterprise without gaps between hosted, on-premise, and cloud?	High	
Single-Pane Correlation	Unified SIEM across all assets, or split across platforms with no cross-correlation?	High	
Hosted Environment Coordination	If you have a hosting provider, does the MSSP coordinate with them — or create a seam in visibility?	High	
INCIDENT RESPONSE & REMEDIATION			
Patient Safety-First Response	Does IR methodology prioritize patient safety when making containment decisions on clinical systems?	High	
Remediation Support	Hands-on remediation, or detection/alerting only? Can they restore operations, not just identify threats?	Med	
Incident Coordination Model	How many vendor handoffs between detection and your team being notified? Fewer layers = faster response.	High	

Key Questions to Ask Every Candidate

1. Who actually operates your SOC? If you use subcontractors or white-label partners, identify them and describe the escalation path during a critical incident.
2. How many healthcare organizations do you serve, and what percentage of your client base is in healthcare? Provide references from hospitals of similar size.
3. Describe your incident response process for ransomware affecting clinical systems. How do you determine which systems to isolate when patient care may be impacted?
4. If we have a hosting relationship with another provider, how does your monitoring integrate with their environment? Will there be a visibility gap at the boundary?
5. Walk us through a recent healthcare incident from detection through remediation. What was the timeline and how did you coordinate with the affected organization?
6. What is your experience with our specific EHR platform? Do your analysts understand its clinical dependencies and traffic patterns?

A NOTE ON TRANSPARENCY

In healthcare, your security provider relationship is a matter of patient safety. Any provider **unwilling to clearly answer** who monitors your environment, how they coordinate with your existing infrastructure, and what happens during a clinical incident **should give you pause**.