Healthcare Cyber Risk Advisory

Protecting Patient Care & Critical Healthcare Operations

Healthcare organizations supporting patient care, EHR systems, clinical operations, and medical technologies operate within a rapidly escalating threat environment. As part of U.S. critical infrastructure, healthcare remains a primary target of nation-state cyber operations.

Recent intelligence confirms a shift. Iran-linked actors have moved beyond ransomware to destructive cyber operations (wiper attacks)—designed to disrupt healthcare delivery, not extort payment.

In a recent attack against a major U.S. healthcare technology company (Stryker), attackers:

- Gained internal access
- Used administrative tools to execute destructive actions
- Wiped systems and reset devices at scale
- Disrupted operations across dependent healthcare environments

There was no ransom. There was no immediate recovery. The objective was disruption.

Operational & Clinical Impact

When these attacks occur:

- EHR access is lost
- Patient care is delayed or diverted
- Clinical operations and scheduling stop
- Billing and revenue cycles halt
- CMS, HIPAA, and compliance exposure increases immediately

Many providers assume they are not a target. They are.

Smaller and mid-sized organizations are frequently treated as soft targets and used as entry points into larger healthcare systems, payer environments, and critical infrastructure networks.

You may not be the primary target. But you are part of the attack path.

Where Exposure Exists

Across healthcare environments, the pattern is consistent:

Leaders believe they are prepared. They are not.

Exposure exists at the intersection of:

- Cybersecurity and IT systems
- Clinical operations and patient care delivery
- Third-party and vendor dependencies
- Business continuity and downtime readiness
- CMS, HHS, and HIPAA compliance requirements

This is not an IT issue. This is a clinical, operational, and regulatory risk. There is no buffer.

72-Hour Executive Risk Review

To address this risk, a limited number of Healthcare Rapid Risk Assessments (72-hour Executive Risk Review) are being conducted to provide a clear, executive-level understanding of:

- Operational disruption exposure across clinical and business systems
- CMS, HIPAA, and Security Risk Assessment (SRA) compliance gaps
- Downtime and business continuity readiness under real conditions
- Third-party, vendor, and supply chain risk exposure
- Definitive answer: Can you sustain clinical operations and remain compliant under disruption?

This is a focused, independent executive assessment—not a long-term engagement—designed to provide immediate clarity.

Investment: $5,500 (Firm Fixed Fee)

Learn more about HCCP by visiting our website or contacting us directly.

Remingio “Remi” Silva, CEO | Phone: (410) 570-9715 | Website: https://hccpros.com/

Focused. Defensible. Audit-Ready.