Cyber Engineering Services

Healthcare-Focused Cyber Expertise to Close the Gap Between Risk and Remediation

Hospitals and health systems often receive Penetration Test or Security Risk Assessment reports identifying critical vulnerabilities—but day-to-day clinical and IT demands delay remediation. CloudWave's Cyber Engineering service bridges this gap by providing healthcare organizations with on-demand access to seasoned cyber engineers who understand the complexity of clinical environments.

Delivered through a flexible block-of-hours model, Cyber Engineering services ensures prioritized, compliant, and well-documented remediation—helping healthcare organizations reduce operational risk while keeping patient care uninterrupted.

SERVICE OBJECTIVES

- **Rapidly remediate findings from Pen Testing and Security Risk Assessments, tailored to healthcare systems and workflows** — reducing the window of exposure and protecting patient safety.

- **Provide hands-on engineering support with deep expertise in hospital IT, cloud, and clinical technologies** — ensuring fixes are implemented correctly the first time and without disrupting clinical operations.

- **Enable flexible consumption of healthcare cyber engineering resources via block hours** — giving hospitals predictable costs and the agility to scale resources as priorities shift.

- **Deliver auditable progress reports that support HIPAA, NIST CSF, and HICP compliance, with Board-level visibility** — providing clear evidence of risk reduction and strengthening governance.

TYPICAL ACTIVITIES

CloudWave's Cyber Engineering service blocks can be applied across a wide range of healthcare-specific remediation needs, including:

- **Identity & Access Hardening:** Active Directory cleanup, MFA rollout across EHR and clinical apps, privileged account remediation

- **Patch & Vulnerability Remediation:** OS/app patching, compensating controls for unpatchable medical devices, risk-based prioritization

- **Network & Perimeter Security:** Firewall optimization, secure segmentation between clinical and administrative networks, remote access protections

- **Cloud Security Engineering:** Correcting misconfigured IAM roles, securing storage for PHI, enabling SOC integration for cloud-hosted EHR workloads

- **Backup & Data Protection:** Encryption, immutability, ransomware recovery validation aligned with hospital disaster recovery needs

- **Logging & Monitoring:** Forwarding and tuning logs from EHRs, endpoints, and cloud platforms to ensure visibility without disrupting workflows

> Delivered through a flexible block-of-hours model, Cyber Engineering services ensures prioritized, compliant, and well-documented remediation—helping healthcare organizations reduce operational risk while keeping patient care uninterrupted.

CloudWave

BLUE ORANGE COMPLIANCE
A CloudWave Company

SERVICE MODEL

- **Base Block:** 25 hours (minimum purchase)
- **Scalable:** Additional 25-hour blocks available as needed
- **Flexible:** Hours may be applied across multiple remediation categories
- **Valid:** 12 months from purchase
- **Transparent:** Progress reports provided at the close of each block

BENEFITS TO HEALTHCARE ORGANIZATIONS

- **Close critical vulnerabilities faster** — minimizing risk to patient safety and protecting sensitive data.
- **Strengthen compliance readiness with documentation mapped to HIPAA, NIST CSF, and HICP** — reducing audit stress and ensuring regulatory alignment.
- **Reduce cyber and operational risk with expertise built on protecting over 300 hospitals and health systems** — leveraging proven healthcare-specific experience.
- **Predictable cost structure with easy scalability** — allowing IT and security leaders to plan budgets while adapting quickly to new threats or findings.
- **Access to CloudWave's dual expertise in healthcare technology and advanced cybersecurity engineering** — ensuring remediation supports both secure operations and uninterrupted care delivery.

SUMMARY

CloudWave's Cyber Engineering service empowers healthcare organizations to move from risk identification to risk resolution—quickly, effectively, and with confidence. With a unique combination of healthcare IT understanding and cybersecurity engineering expertise, Cyber Engineering services enables hospitals to remediate vulnerabilities without overburdening staff or disrupting patient care.

PROTECTING

300+

HOSPITALS AND HEALTH SYSTEMS

HEALTHCARE TECHNOLOGY

STRENGTHEN COMPLIANCE

CYBERSECURITY ENGINEERING

ABOUT CLOUDWAVE

CloudWave is a full-service cybersecurity and cloud services provider built exclusively for healthcare. Protecting over 350 hospitals and health system environments, CloudWave delivers end-to-end solutions that combine secure hosting, IT operations, and 24/7 threat detection and response. Services include managed security, risk and compliance, disaster recovery, systems management, and cloud optimization—all delivered with a healthcare-first mindset. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Centers, CloudWave provides a cyber-ready foundation for safe, uninterrupted patient care.

ABOUT BLUEORANGE COMPLIANCE

BlueOrange Compliance, a CloudWave company, is a leader in information privacy and security, regulatory compliance, and risk management services. Together with CloudWave, BlueOrange Compliance delivers end-to-end cybersecurity solutions for healthcare organizations facing increasingly complex compliance landscapes, including HIPAA, HITECH, OCR, and other industry-specific regulations.

The combination of our proven track record in compliance audits, risk assessments, cybersecurity testing and training, and cybersecurity consulting and risk management services along with CloudWave's advanced threat detection, incident response, and cloud infrastructure capabilities results in a comprehensive set of offerings that empower healthcare organizations to secure sensitive data, streamline compliance efforts, and mitigate evolving cyber threats.

gocloudwave.com | **blueorangecompliance.com**