BEACON
HEALTHCARE SYSTEMS

Fast-growing Healthcare SaaS Compliance Solution provider in the Medicare/Medicaid/Commercial space is seeking a Project Manager to join our team.

Who We Are:

Beacon Healthcare Systems Inc. is an exciting software as a service (SaaS) company thriving in the healthcare space. We provide compliance and regulatory software modules for applicable stakeholders in the health insurance industry.

Why Work Here?

- Lead meaningful projects that directly impact compliance outcomes for health plans across the country.
- Work in a dynamic, fast-growing SaaS environment where your organizational skills make a real difference.
- Collaborate across engineering, product, sales, and customer success teams on high-visibility initiatives.
- Competitive compensation, remote flexibility, and a mission-driven team that values your contributions.

Role: Director of Cybersecurity and Compliance

Location: May telecommute 90% of the workweek from any U.S. location

Compensation: $164,798 per year along with standard employee benefits

Description:

Leverage advanced knowledge of computer science and cybersecurity to develop, implement, and lead the organization's cybersecurity strategy, with a focus on migrating from a private data center to AWS Cloud while maintaining HITRUST, SOC 2, and HIPAA compliance. Specific duties include:

- Develop and execute a comprehensive cybersecurity strategy, ensuring alignment with business objectives and regulatory compliance requirements with HITRUST, SOC 2, HIPAA, NIST 800-53, and ISO 27001 security frameworks.
- Provide strategic guidance to the executive leadership team on cybersecurity risks, threats, and investment priorities.

- Establish and manage the Security Governance Committee, ensuring ongoing oversight of security programs and incident response readiness and define security metrics and KPIs, reporting security posture and risk trends to executive stakeholders.
- Lead the secure migration initiative from a private data center to AWS Cloud, ensuring security best practices are embedded into the architecture.
- Design and implement AWS networking and security controls, including VPC configurations, security groups, IAM policies, Transit Gateway, and Direct Connect.
- Monitor and enforce network segmentation, firewall configurations, and VPN solutions for secure connectivity.
- Develop policies for data residency, cross-border data transfer, and encryption, ensuring regulatory adherence.
- Develop and enforce an Incident Response Plan (IRP), ensuring rapid containment and forensic investigation of cyber threats.
- Conduct tabletop exercises, red team/blue team simulations, and phishing attack drills to enhance security preparedness and implement end-to-end encryption strategies, using AWS KMS, customer-managed keys (CMKs), and envelope encryption.
- Deploy Data Loss Prevention (DLP) solutions for cloud storage, databases, and SaaS applications.
- Design cloud backup and disaster recovery solutions, ensuring resilience against ransomware and data loss events.
- Provide CTO-level security briefings to executive leadership, ensuring informed decision-making on cyber risks.
- Lead cybersecurity strategy sessions, working with legal, compliance, and IT teams to align security initiatives with business goals.
- Will supervise a team of 6 professional employees with titles including DevOps Engineer; Systems Engineer; Cloud Architect; Penetration Tester; and SOC Manager.

Minimum Requirements: Master's degree or foreign equivalent degree in Computer Science, Cybersecurity, or directly related quantitative field plus two (2) years of relevant professional experience conducting various cybersecurity, information security technical duties. Experience must include each of the following, which may be gained concurrently before, during, or after completion of advanced degree:

- 2 years of experience with identity and access management, vulnerability management, penetration Testing, IT Security governance and compliance, and IT security disaster recovery;
- 2 years of experience with HIPAA, HITRUST CSF, and ISE/IEC 27001 compliance regulations;
- 2 years of experience budgeting and conducting resource allocation for cybersecurity initiatives;

- 2 years of experience utilizing SIEM Solutions, including Splunk, QRadar, and Microsoft Sentinel;
- 2 years of experience with cloud security programs including AWS Security Hub, Azure Security Center, and Google Chronicle.

Job site: 17011 Beach Blvd, Suite 1220, Huntington Beach, CA 92647.
40 hours per week, 9:00am to 5:00pm.
Send resume to:
Beacon Healthcare Systems, Inc
Attn: Chris Mahoney, Chief Financial Officer
17011 Beach Blvd, Suite 1220, Huntington Beach, CA 92647

Beacon Healthcare Systems is proudly an equal opportunity employer. The company is headquartered in Huntington Beach, CA