Job Title: Cybersecurity and Device Integration Analyst – Medical Devices

Department: Healthcare Technology Management (HTM) Services

Reports To: Clinical Engineering Manager / HTM Program Manager

FLSA Status: Exempt / Salary

Position Summary

The Cybersecurity and Device Integration Analyst supports the secure operation, connectivity, and lifecycle management of networked medical devices and systems across client healthcare facilities. This role focuses on identifying, assessing, mitigating, and monitoring cybersecurity risks within the medical device ecosystem while supporting safe and effective integration with clinical and IT infrastructure. The analyst works collaboratively with HTM, IT, and Information Security teams to ensure that all connected devices comply with regulatory standards, hospital security policies, and industry best practices.

Key Responsibilities

- Support the development, implementation, and maintenance of cybersecurity programs specific to medical devices and clinical systems.
- Perform risk assessments and vulnerability analyses on network-connected medical equipment.
- Collaborate with hospital Information Security and IT departments to segment, monitor, and secure medical device networks.
- Evaluate medical device configurations, firmware versions, and software updates for security compliance and compatibility.
- Assist in incident response investigations related to medical device cybersecurity events.
- Maintain and update an accurate medical device inventory including IP addresses, software versions, and security patch levels.
- Support integration projects by coordinating with OEMs, HTM staff, and hospital IT to ensure safe and compliant device connectivity.
- Monitor threat intelligence sources and regulatory advisories (e.g., FDA, ICS-CERT, H-ISAC) to identify potential risks to deployed medical technologies.
- Document findings, risk mitigation plans, and compliance reports for leadership and regulatory review.
- Provide training and awareness to HTM and clinical staff regarding cybersecurity practices, policies, and incident reporting procedures.

- Assist with implementation of medical device cybersecurity standards such as AAMI TIR57, TIR97, and FDA postmarket guidance.
- Contribute to continuous improvement initiatives for device integration, asset management, and cybersecurity defense.

Qualifications

Education & Experience:

- Bachelor's degree in Biomedical Engineering, Information Technology, Cybersecurity, Computer Science, or related field required.
- Minimum of 3 years of experience supporting medical device integration, cybersecurity, or clinical IT systems.
- Experience in hospital or HTM service environments strongly preferred.

Certifications (Preferred):

- CompTIA Security+, Network+, or CySA+
- Certified Information Systems Security Professional (CISSP) or Certified Biomedical Equipment Technician (CBET) a plus
- Certified Healthcare Technology Manager (CHTM) or Certified Information Systems Auditor (CISA) beneficial

Knowledge & Skills:

- Solid understanding of cybersecurity principles, networking protocols, and medical device communication standards (DICOM, HL7, IEEE 11073).
- Familiarity with clinical device integration architectures and medical device data systems.
- Experience with vulnerability management tools, network monitoring systems, and endpoint protection solutions.
- Knowledge of FDA medical device cybersecurity guidance, HIPAA security requirements, and NIST Cybersecurity Framework.
- Strong analytical and problem-solving abilities with attention to technical detail.
- Excellent communication skills for working across clinical, technical, and administrative teams.
- Ability to manage multiple projects while maintaining compliance documentation and timely reporting.

Physical Requirements

- Ability to move freely throughout healthcare facilities and technical environments.

- Occasional lifting of up to 25 lbs. of tools or equipment.
- Periodic travel to other client sites for audits, assessments, or projects.

Work Environment

- Hospital and healthcare IT environments, including data centers, clinical departments, and administrative offices.
- Exposure to networked medical systems and sensitive healthcare data (under strict confidentiality protocols).
- Collaborative, project-driven setting requiring professionalism, adaptability, and discretion.

About the Company

ELITE Healthcare Technology Resources is a third-party Healthcare Technology Management (HTM) service provider specializing in medical and diagnostic equipment management, cybersecurity, and technology integration. We partner with hospitals and healthcare organizations to deliver secure, reliable, and regulatory-compliant technology solutions that enhance patient care, data protection, and operational performance.