**Position Title:** Security Analyst – Project REACH
**Location:** Bayview Campus
**Reports to:** HIS Project Director, Technology, Infrastructure, Devices

**Position Summary:**

Sunnybrook Health Sciences Centre is a nationally and internationally recognized academic health centre with multiple sites across the Greater Toronto Area (GTA). We provide expert, compassionate care to patients across Ontario, deliver broad and specialized education to thousands of learners, and lead cutting-edge research that shapes the future of healthcare.

As part of a major digital and clinical transformation, Sunnybrook is launching Project REACH, a multi-year initiative to implement a new health information system (HIS) across all campuses and satellite sites. Project REACH is rooted in clinical transformation and care redesign. Led by the Clinical Informatics Team, the project aims to enhance patient care, improve clinical workflows, and better support our care teams.

**Overview:** Reporting to the HIS Project Director, Technology, Infrastructure, Devices, the Security Analyst will support cybersecurity activities related to the implementation of a new Health Information System (HIS) across a multi-site hospital environment. Sunnybrook is seeking a skilled and proactive **Cybersecurity and Cloud Security Analyst** to support the secure implementation and deployment of a new **Health Information System (HIS)**. This role is critical in ensuring the confidentiality, integrity, and availability of patient data and health records during the migration, deployment, and ongoing management of HIS infrastructure—both on-premises and in the cloud. This role is responsible for ensuring appropriate access controls, conducting risk assessments, supporting vulnerability management, and ensuring HIS security design aligns with regulatory, organizational, and industry best practices.

**Key Responsibilities:**

* Collaborate with IT, vendors, and project managers to develop and enforce security controls for the new HIS infrastructure.
* Collaborate with technical and project teams to ensure secure design, implementation, and deployment of HIS components in alignment with best practice and Hospital cyber controls.
* Design and implement a security framework aligned with the NIST Cybersecurity Framework (CSF) to protect patient health information (PHI).
* Assess cloud security posture and implement necessary configurations, controls, and monitoring for HIS workloads.
* Conduct threat modeling, risk assessments, and vulnerability assessments on HIS components and associated systems.
* Manage identity and access control (IAM), multi-factor authentication (MFA), and role-based access for HIS users.
* Monitor cloud environments and network traffic for anomalies, threats, or unauthorized access attempts during and after implementation.
* Ensure all HIS data transfers, APIs, and integrations are encrypted and securely configured.
* Lead security incident response planning and support incident handling related to HIS.
* Review third-party vendor security documentation and perform due diligence on HIS SaaS or PaaS providers.
* Create and maintain documentation for security policies, procedures, risk registers, and audit logs.
* Support audit readiness and compliance reporting for HIS systems.

**Qualifications:**

**Education:**

* Bachelor’s degree in Cybersecurity, Information Systems, Computer Science, or related field.
* Relevant certifications preferred: CISSP, CCSP, CISA, HCISPP, CEH, or similar.

**Experience:**

* 3–5 years of experience in cybersecurity, including 1–2 years of cloud security.
* Hands-on experience with securing Electronic Health Records (EHR) or Health Information Systems (HIS).
* Familiarity with HIPAA, HITECH, NIST Cybersecurity Framework, and other healthcare compliance regulations.
* Experience with cloud security tools and architecture.
* Knowledge of secure DevOps (DevSecOps) practices is a plus.

**Technical Skills:**

* Proficiency in SIEM tools, endpoint detection & response (EDR), and vulnerability scanning tools.
* Experience with cloud-native security services (e.g., AWS Security Hub, Azure Defender).
* Strong understanding of network security, firewalls, IDS/IPS, and encryption protocols.

**Preferred:**

* Prior experience in a healthcare or hospital IT environment.
* Involvement in large-scale HIS or EMR implementations such as Epic, Cerner, MEDITECH, etc.
* Knowledge of healthcare interoperability standards (e.g., HL7, FHIR).