Job Title: Chief Information Security Officer

Department: Information Technology Department

Reports To: Senior Vice President, Chief Information Officer

FTE: Full-Time

About Healthix:

Healthix is part of a nationwide movement to improve our health care system through better access to information. Healthix is the largest public health information exchange (HIE) in the nation, bringing together over 600 healthcare organizations at more than 6,000 sites across New York City and Long Island. We provide secure access to clinical data of more than 16 million patients to improve quality of care, efficiency and effectiveness. Healthix delivers actionable patient data electronically 24/7 in real time, with patient consent and consistent with regulations and policies established by NY State Department of Health. Healthix mission is to support healthcare providers and health plans to provide care management, improve clinical outcomes, promote efficiency and reduce healthcare costs.

Position Summary:

Reporting to the Senior Vice President and Chief Information Officer, the Chief Information Security Officer (CISO) plays an integral part in defining the fundamental principles for the protection of Healthix's information resources and the proper controls needed to ensure compliance with internal and external regulations, while supporting the business needs and upholding the Healthix's reputation with its participants.

The Chief information Security Officer will be accountable to oversee all the Information Security policies and procedures in place and determine the security controls that are appropriate to the level of risk associated with IT systems leveraged to support Healthix employees and customer services. This role will provide strategic leadership and lead an Information Security program to manage and improve information security while mitigating risk.

This role serves as an expert advisor to senior management in the development, implementation and maintenance of information systems to ensure that best practice control objectives are achieved in protecting information assets.

The candidate will guide the senior leadership team by making pragmatic recommendations for priority investments and projects that will mitigate overall risks by strengthening defenses and reducing vulnerabilities for Healthix's information assets.

Responsibilities include but are not limited to:

- Lead and facilitate Healthix's Security Committee, chaired by a Healthix Board Member, to update and work with customer CISOs as advisors to Healthix security activities
- Direct the preparation activities to support HITRUST and MARS-E audits
- Develop, manage and improve a comprehensive information security risk-based program to ensure the integrity, confidentiality and availability of information assets.
- Develop an IT security architecture roadmap that will identify security controls, and identify and assess technologies that will enforce the organization's security priorities.
- Develop, maintain, and promote information security policies, standards and guidelines. Ensure that controls comply with contractual obligations, corporate policies, and legal and regulatory requirements.
- Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users.
- Define and facilitate the information security risk assessment process, including the reporting and oversight of treatment efforts to address findings with collaboration of the Sr. Director of Compliance and Compliance Coordinators.
- Create, communicate and implement a process to manage vendor risk, including assessment and remediation efforts to address such risks that may result from partners, consultants and other service providers.
- Provide strategic risk guidance and consultation for corporate IT projects, including the evaluation and recommendation of technical standards and controls.
- Establish and implement a process for incident management to effectively identify, respond, contain and communicate a suspected or confirmed incident with collaboration of the Sr. Director of Compliance and Compliance Coordinators.
- Identify, assess, and prioritize IT risks to corporate data and systems, including external threats, cyber-crimes, internal threats and third-party risks. Advise relevant stakeholders on the appropriate courses of action to mitigate or eliminate risk.
- Coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of a security event. Provide direction, support and in-house consulting in these areas.

- Effectively manage an information security budget, and monitor for variances.

- Provide regular reporting on the current status of the information security program to the senior leadership team and the board of directors as part of a strategic enterprise risk management program.

- Facilitate a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the security.

The qualified candidate for this position will possess:

Education:
Bachelor degree in Information Security, Computer Science, Management of Information Systems, or related field required. Masters preferred.

Experience:

Minimum of 8 years of experience in a combination of risk management, information security and information technology fields. At least 4 years of experience in a senior leadership role. Employment history must demonstrate increasing levels of responsibility.

Required Skills and Abilities:

- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and nontechnical audiences.

- Proven track record and experience in developing information security policies and procedures, as well as successfully executing programs that meet the objectives of excellence in a dynamic environment.

- Poise and ability to act calmly and competently in high-pressure, high-stress situations.

- Knowledge and demonstrated experience of relevant legal and regulatory requirements, such as HITRUST, MARS-E, SOX, PCI DSS, HITECH, HIPAA Privacy & Security and other CMS regulations and guidelines as they are updated by the Federal Government.

- Knowledge of common information security management frameworks, such as NIST.

- Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.

- Knowledge of various health care related code sets such as CPT-4, ICD-9/10, LOINC, SNOMED, etc.

- Exhibit excellent analytical skills, the ability to manage multiple, inter-disciplinary projects as well as the ability to work well in a demanding, dynamic environment and meet overall objectives.

- Project management skills: financial/budget management, scheduling and resource management.

- Prominent level of personal integrity, as well as the ability to professionally handle confidential matters, and show an appropriate level of judgment and maturity.

- High degree of initiative, dependability and ability to work with little supervision.

Application:

Interested individuals are invited to apply at careers@heatlhix.org.